E[redacted]2176640US

WO 01/10079
PCT/KR00/00811

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:
SOHN, Chang, Kyu
401 In-bong Building
640-21, Yoksam-dong
Kangnam-gu
Seoul 135-080
RÉPUBLIQUE DE CORÉE

Date of mailing (day/month/year)	
08 February 2001 (08.02.01)	
Applicant's or agent's file reference	**IMPORTANT NOTICE**
ALOP11	

International application No.	International filing date (day/month/year)	Priority date (day/month/year)
PCT/KR00/00811	27 July 2000 (27.07.00)	29 July 1999 (29.07.99)

Applicant
SAFE TECHNOLOGY CO., LTD. et al

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
   KR,US

   In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
   CN,EP,JP,RU

   The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
   08 February 2001 (08.02.01) under No. WO 01/10079

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a demand for international preliminary examination must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the national phase, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer
J. Zahra

Telephone No. (41-22) 338.83.38

[redacted] [redacted] L652176640US

특 허 협 력 조 약
(PATENT COOPERATION TREATY)

발신:수리관청

수신:

SOHN, Chang Kyu

401, In-Bong Bldg., 640-21 Yoksam-dong, Kangnam-gu, Seoul 135-909, Republic of Korea

PCT

국제출원번호 및 국제출원일 통지서

(PCT 규칙 20.5(C))

발송일 (일/월/년)	05 AUGUST 2000 (05.08.2000)
출원인 또는 대리인의 서류참조기호 ALOP11	중요통지사항

국제출원번호	국제출원일 (일/월/년)	우선일 (일/월/년)
PCT/KR00/00811	27 JULY 2000 (27.07.2000)	29 JULY 1999 (29.07.1999)

출원인

SAFE TECHNOLOGY CO., LTD et al

발명의 명칭

ADAPTER HAVING SECURE FUNCTION AND COMPUTER SECURE SYSTEM USING IT

1. 이 국제출원은 위에 기재된 바와 같이 국제출원번호와 국제출원일이 부여되었습니다.

2. 이 국제출원의 기록원본은:

☐ _____ 자로 국제사무국에 송부되었습니다.

☐ 아래의 사유로 인하여 아직 국제사무국에 송부되지 않았으며, 이 통지서의 사본은 국제사무국에 송부되었습니다*:

☐ 국가안전보장에 필요한 허가를 얻지 못했음

☐ 기타 (이유를 상술):

* 국제사무국은 수리관청에 의한 기록원본의 송달을 감시하고 그 접수사실을 출원인에게 통지합니다. (서식 PCT/IB/301). 국제사무국은 우선일부터 14월이 경과할 때까지 기록원본을 수령하지 않은 때에는 출원인에게 이를 통지합니다. (규칙 22.1(c)).

수리관청명칭 및 우편주소 Korean Industrial Property Office Government Complex-Taejon, Dunsan-dong, So-ku, Taejon Metropolitan City 302-701, Republic of Korea 팩스번호: 82-42-472-3466	특허청장 COMMISSIONER 전화번호: 82-42-481-5207

서식 PCT/RO/105 (1992년 7월)

PCT REQUEST ALOP11

RECORD COPY

Original (for **SUBMISSION**) - printed on 27.07.2000 02:27:36 PM

0	**For receiving Office use only**	
0-1	International Application No.	PCT/KR 00/00811
0-2	International Filing Date	27 July 2000 (27.07.00)
0-3	Name of receiving Office and "PCT International Application"	Korean Industrial Property Office PCT International Application
0-4	**Form - PCT/RO/101 PCT Request**	
0-4-1	Prepared using	PCT-EASY Version 2.91 (updated 01.07.2000)
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	Korean Industrial Property Office (RO/KR)
0-7	**Applicant's or agent's file reference**	ALOP11
I	**Title of invention**	ADAPTER HAVING SECURE FUNCTION AND COMPUTER SECURE SYSTEM USING IT
II	**Applicant**	
II-1	This person is:	applicant only
II-2	Applicant for	all designated States except US
II-4	Name	SAFE TECHNOLOGY CO., LTD
II-5	Address:	4F, Union Building 48-18, Songpa-Dong, Songpa-Gu 138-070 Seoul Republic of Korea
II-6	State of nationality	KR
II-7	State of residence	KR
II-8	Telephone No.	82-2-3431-2951
II-9	Facsimile No.	82-2-3431-2056
II-10	e-mail	jwl@esafetek.com
III-1	**Applicant and/or inventor**	
III-1-1	This person is:	applicant and inventor
III-1-2	Applicant for	US only
III-1-4	Name (LAST, First)	LEE, Jong Woo
III-1-5	Address:	101-901, Hansung Apt., 698-2, Pungduckchun-ri, Suji-eub, Yongin-si 449-840 Kyeongki-do Republic of Korea
III-1-6	State of nationality	KR
III-1-7	State of residence	KR

PCT REQUEST

ALOP11

Original (for **SUBMISSION**) - printed on 27.07.2000 02:27:36 PM

IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name (LAST, First)	SOHN, Chang Kyu
IV-1-2	Address:	401, In-bong Bldg., 640-21, Yoksam-dong, Kangnam-gu 135-080 Seoul Republic of Korea
IV-1-3	Telephone No.	82-2-555-2596,2597
IV-1-4	Facsimile No.	82-2-555-2598
IV-1-5	e-mail	ckstpi@hananet.net
V	**Designation of States**	
V-1	Regional Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE and any other State which is a Contracting State of the European Patent Convention and of the PCT
V-2	National Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	CN JP KR RU US
V-5	**Precautionary Designation Statement** In addition to the designations made under items V-1, V-2 and V-3, the applicant also makes under Rule 4.9(b) all designations which would be permitted under the PCT except any designation(s) of the State(s) indicated under item V-6 below. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit.	
V-6	**Exclusion(s) from precautionary designations**	NONE
VI-1	**Priority claim of earlier national application**	
VI-1-1	Filing date	29 July 1999 (29.07.1999)
VI-1-2	Number	10-1999-0031145
VI-1-3	Country	KR
VI-2	**Priority document request** The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s):	VI-1
VII-1	**International Searching Authority Chosen**	Korean Industrial Property Office (KIPO) (ISA/KR)

RECEIVED BY RO

PCT REQUEST ALOP11

Original (for **SUBMISSION**) - printed on 27.07.2000 02:27:36 PM

VIII	Check list	number of sheets	electronic file(s) attached
VIII-1	Request	3	-
VIII-2	Description	18	-
VIII-3	Claims	5	-
VIII-4	Abstract	1	-
VIII-5	Drawings	9	-
VIII-7	TOTAL	36	
	Accompanying items	paper document(s) attached	electronic file(s) attached
VIII-8	Fee calculation sheet	✓	-
VIII-16	PCT-EASY diskette	-	diskette
VIII-18	**Figure of the drawings which should accompany the abstract**	1	
VIII-19	**Language of filing of the international application**	Korean	
IX-1	**Signature of applicant or agent**		
IX-1-1	Name (LAST, First)	SOHN, Chang Kyu	

FOR RECEIVING OFFICE USE ONLY

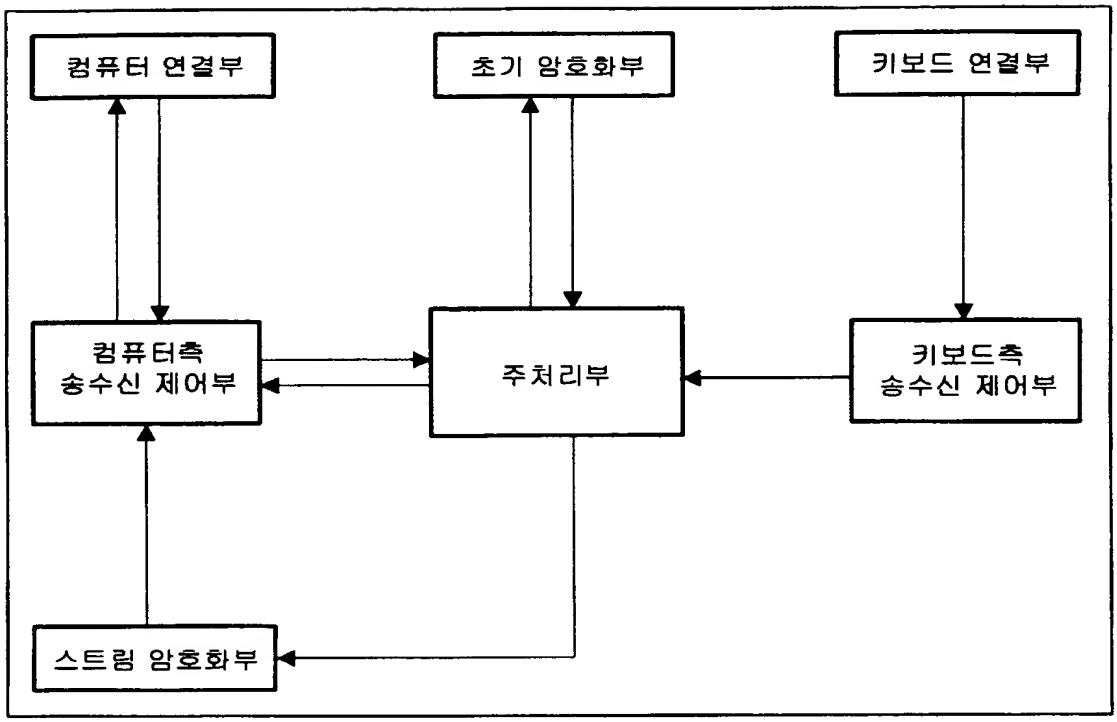
10-1	**Date of actual receipt of the purported international application**	27 July 2000 (27.07.00)
10-2	**Drawings:**	
10-2-1	Received	
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	ISA/KR
10-6	**Transmittal of search copy delayed until search fee is paid**	

FOR INTERNATIONAL BUREAU USE ONLY

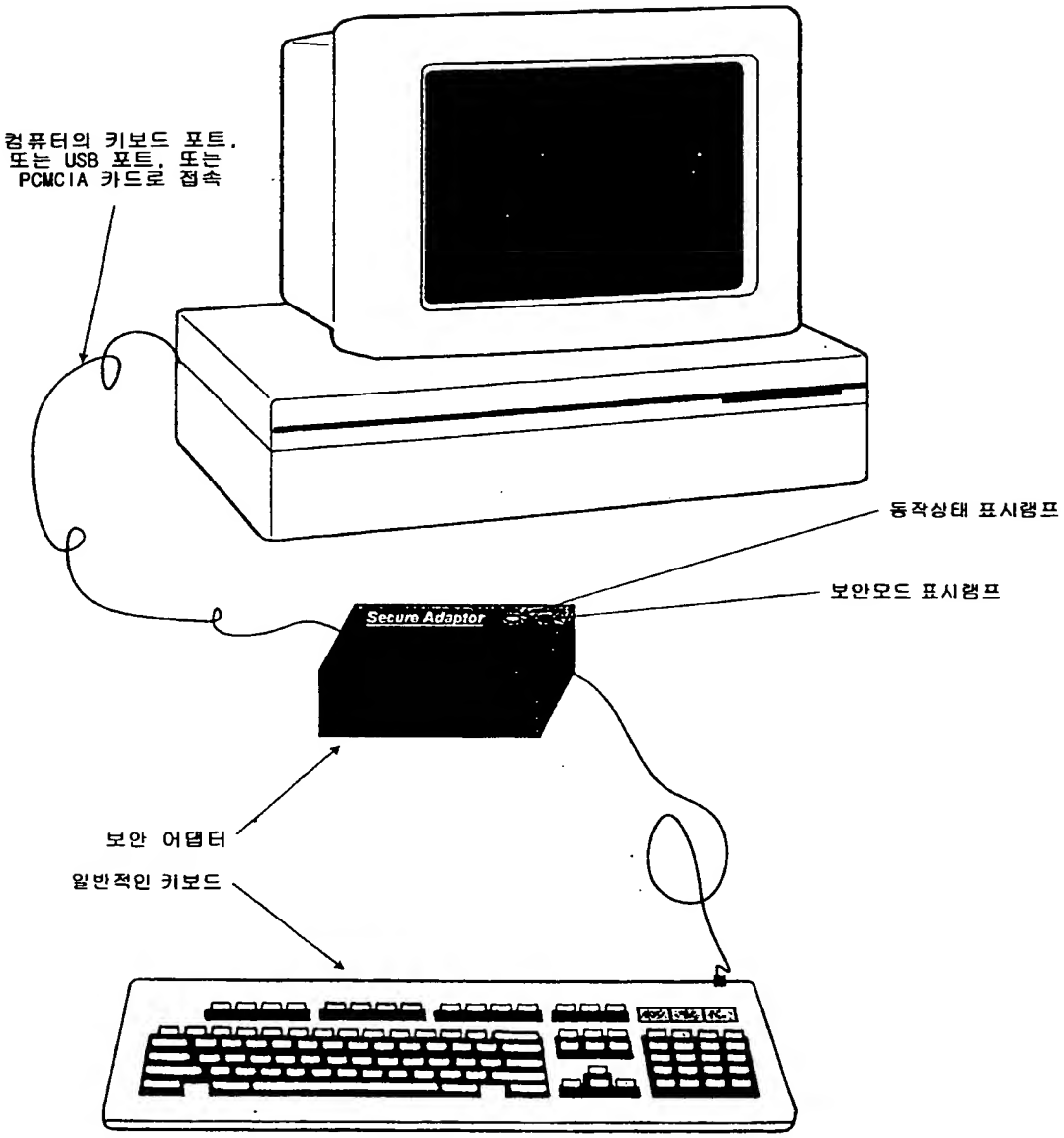
11-1	**Date of receipt of the record copy by the International Bureau**	15 AUGUST 2000 (15.08.00)

【도면】

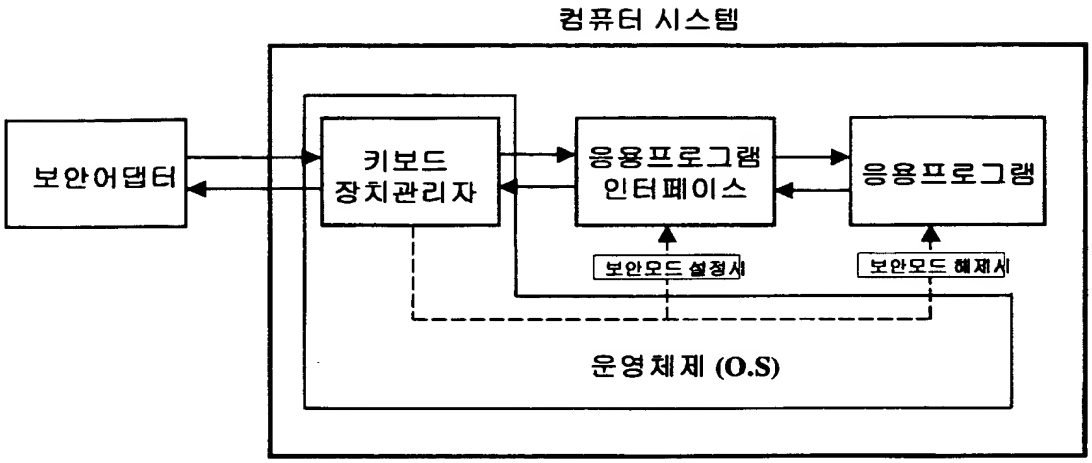
【도 1】



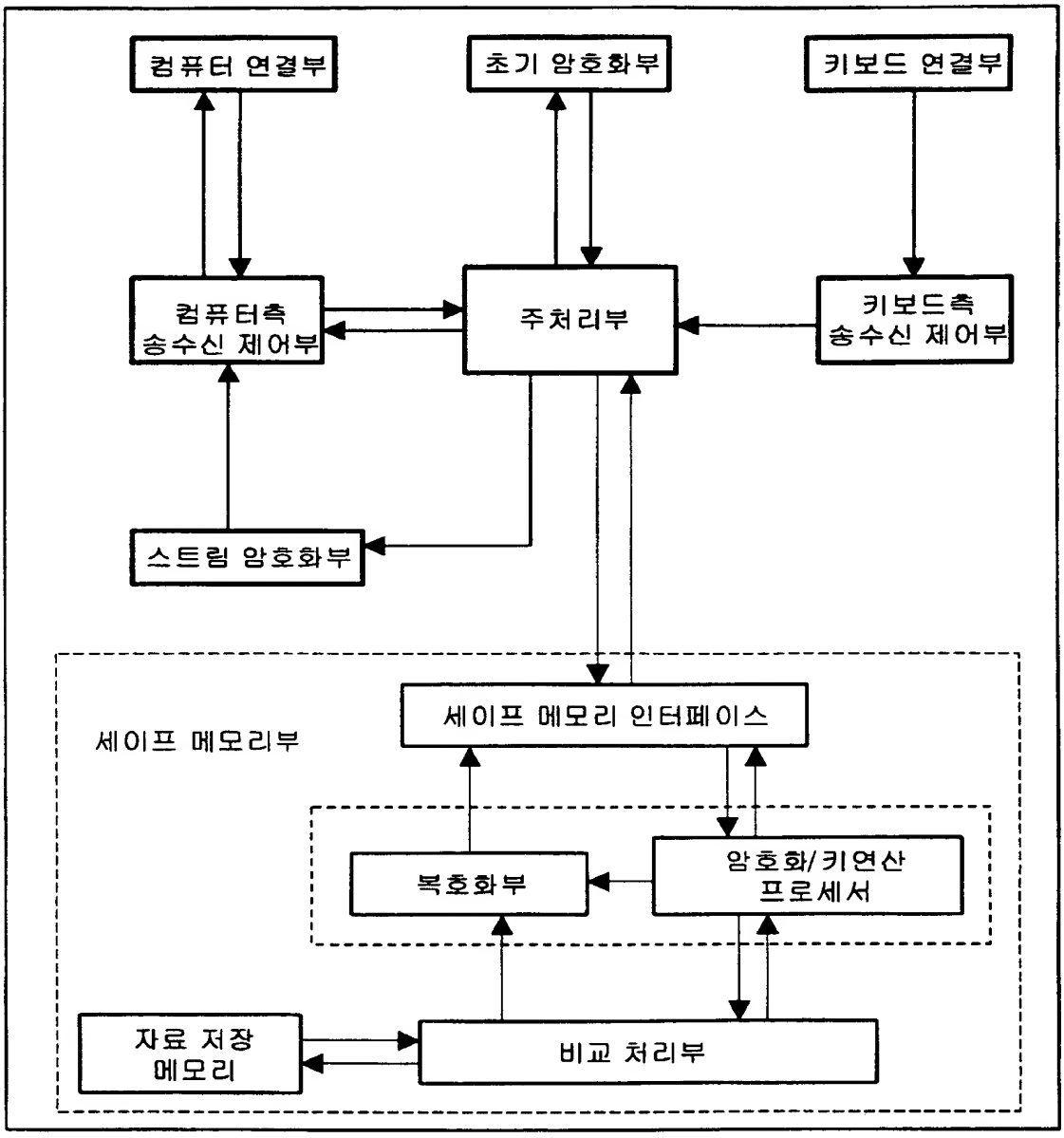
【도 2】


컴퓨터의 키보드 포트,
또는 USB 포트, 또는
PCMCIA 카드로 접속
동작상태 표시램프
보안모드 표시램프
Secure Adaptor
보안 어댑터
일반적인 키보드

【도 3】

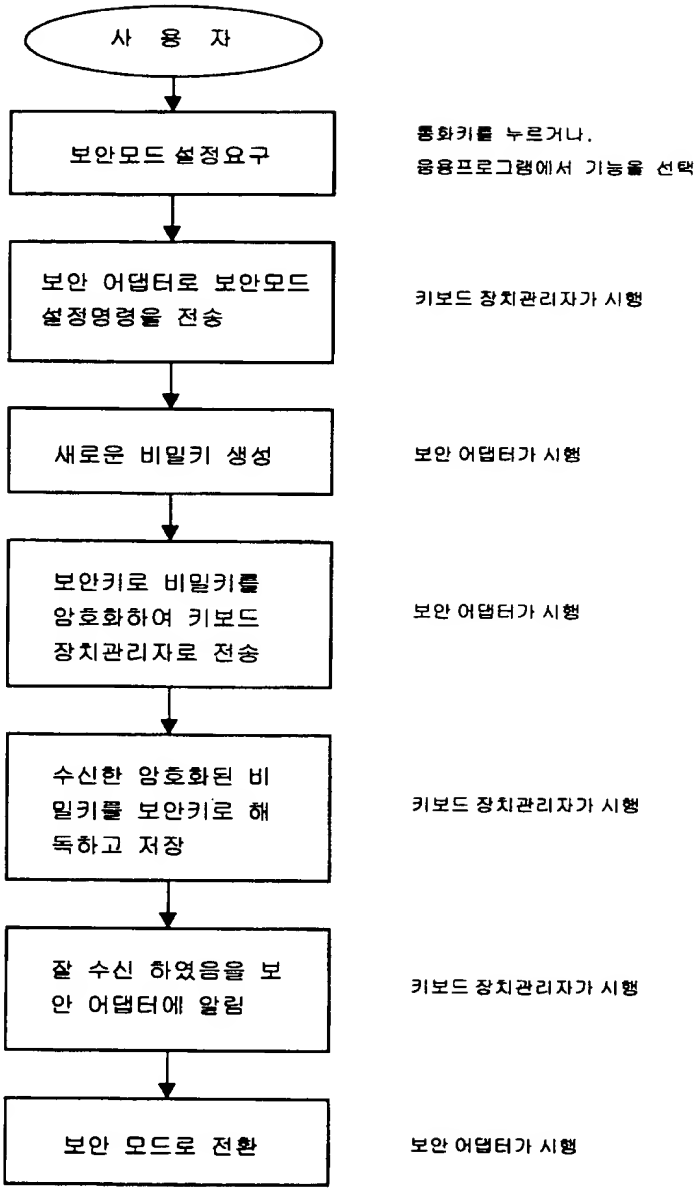

컴퓨터 시스템
보안어댑터
키보드
장치관리자
응용프로그램
인터페이스
응용프로그램
보안모드 설정시
보안모드 해제시
운영체제 (O.S)

【도 4】

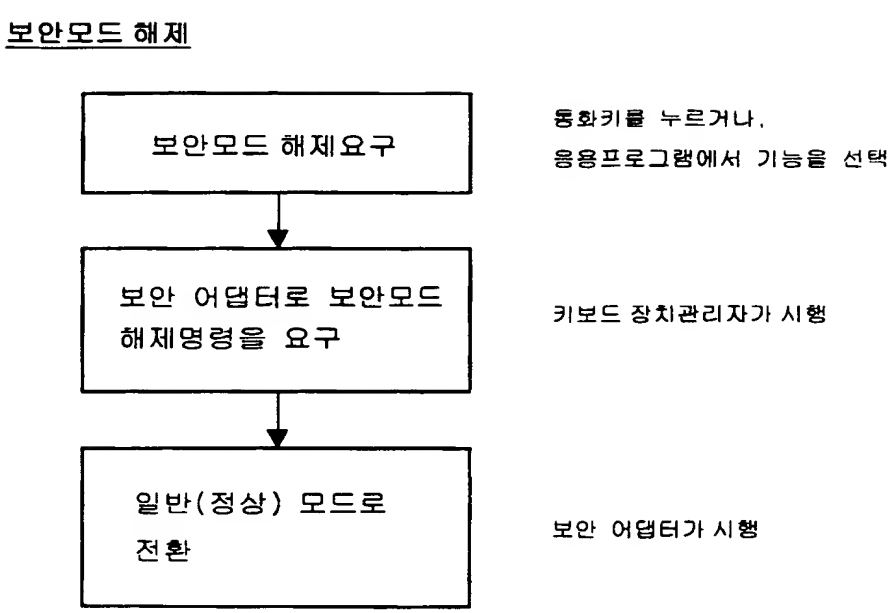

컴퓨터 연결부
초기 암호화부
키보드 연결부
컴퓨터측
송수신 제어부
주처리부
키보드측
송수신 제어부
스트림 암호화부
세이프 메모리부
세이프 메모리 인터페이스
복호화부
암호화/키연산
프로세서
자료 저장
메모리
비교 처리부

【도 5】

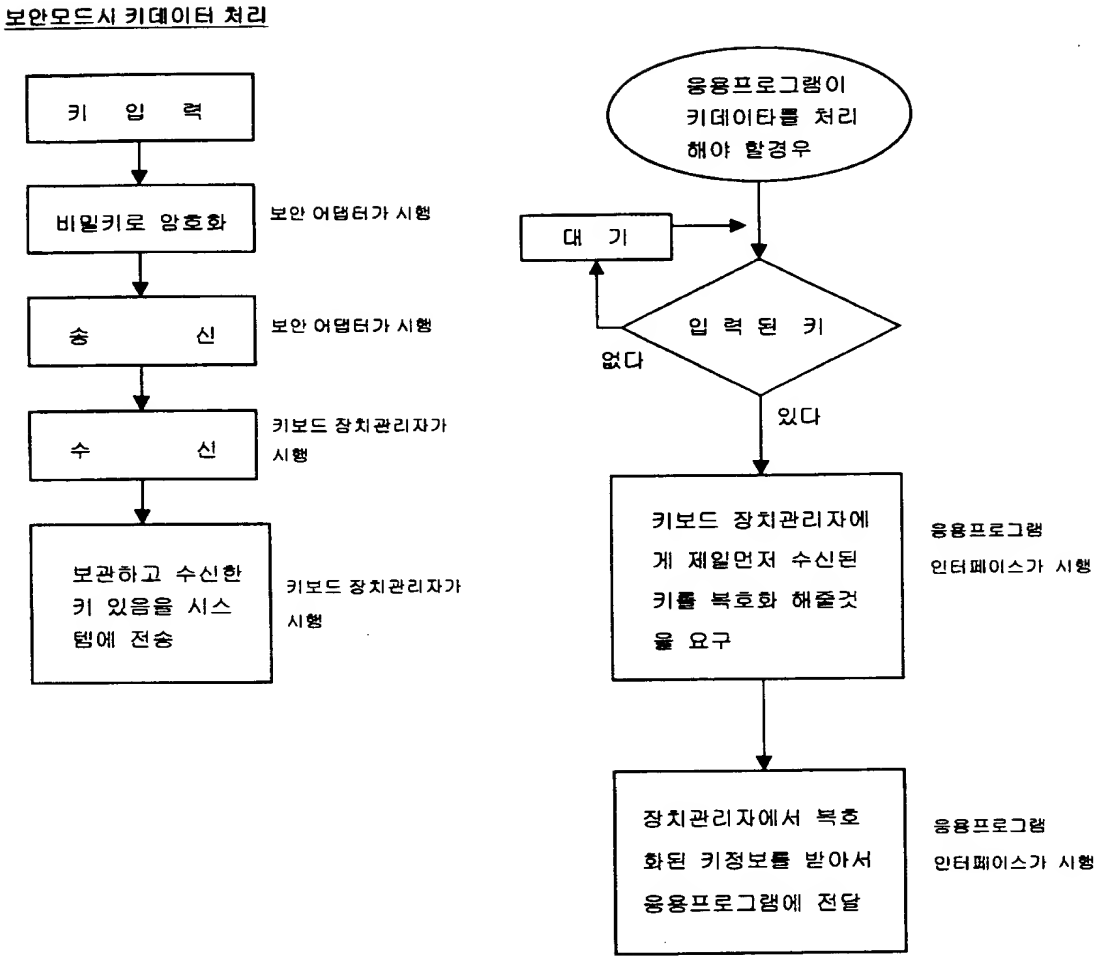
보안모드 설정


사 용 자
보안모드 설정요구
통화키를 누르거나,
응용프로그램에서 기능을 선택
보안 어댑터로 보안모드
설정명령을 전송
키보드 장치관리자가 시행
새로운 비밀키 생성
보안 어댑터가 시행
보안키로 비밀키를
암호화하여 키보드
장치관리자로 전송
보안 어댑터가 시행
수신한 암호화된 비
밀키를 보안키로 해
독하고 저장
키보드 장치관리자가 시행
잘 수신 하였음을 보
안 어댑터에 알림
키보드 장치관리자가 시행
보안 모드로 전환
보안 어댑터가 시행

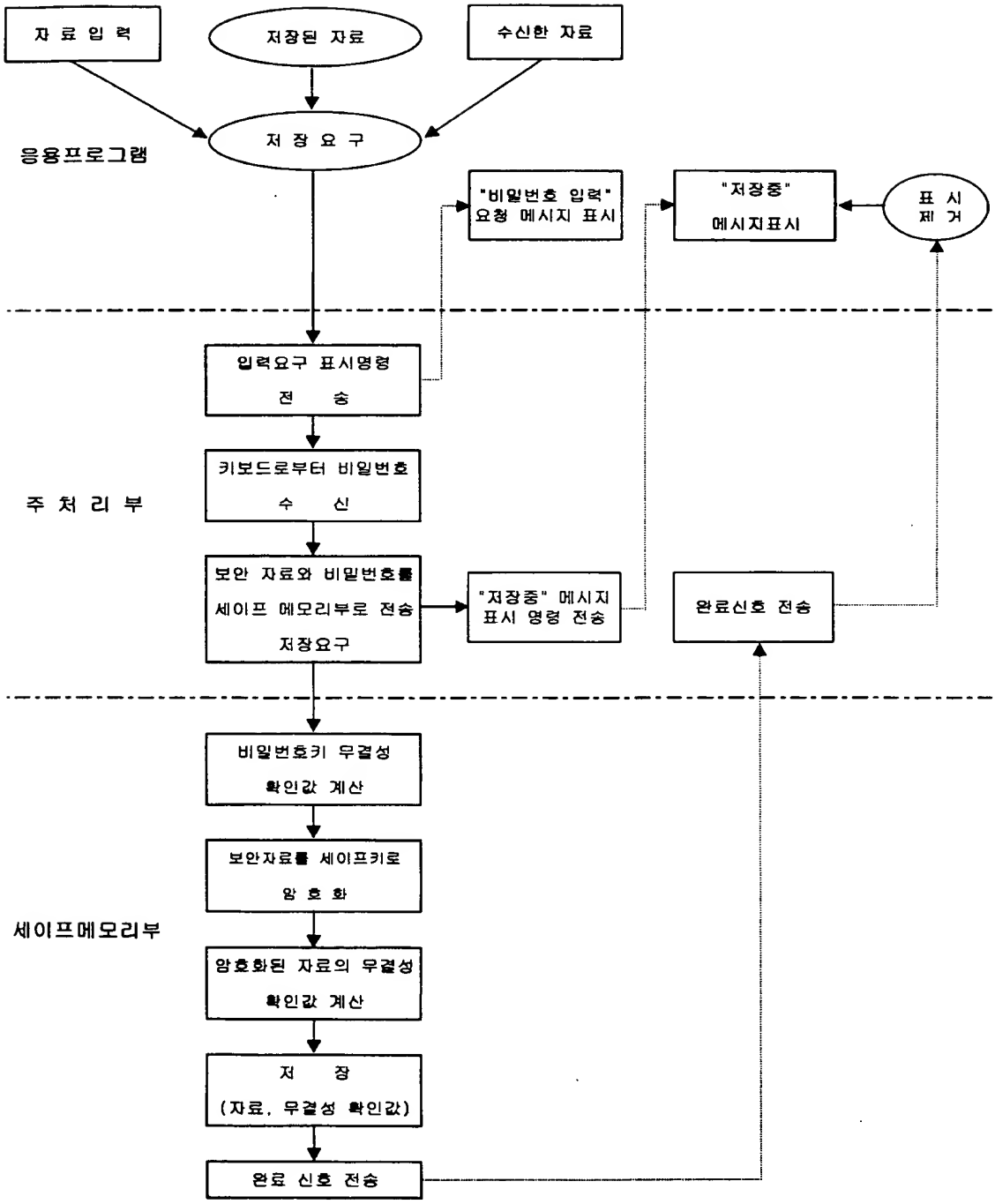
【도 6】


보안모드 해제
보안모드 해제요구
동화키를 누르거나,
응용프로그램에서 기능을 선택
보안 어댑터로 보안모드
해제명령을 요구
키보드 장치관리자가 시행
일반(정상) 모드로
전환
보안 어댑터가 시행

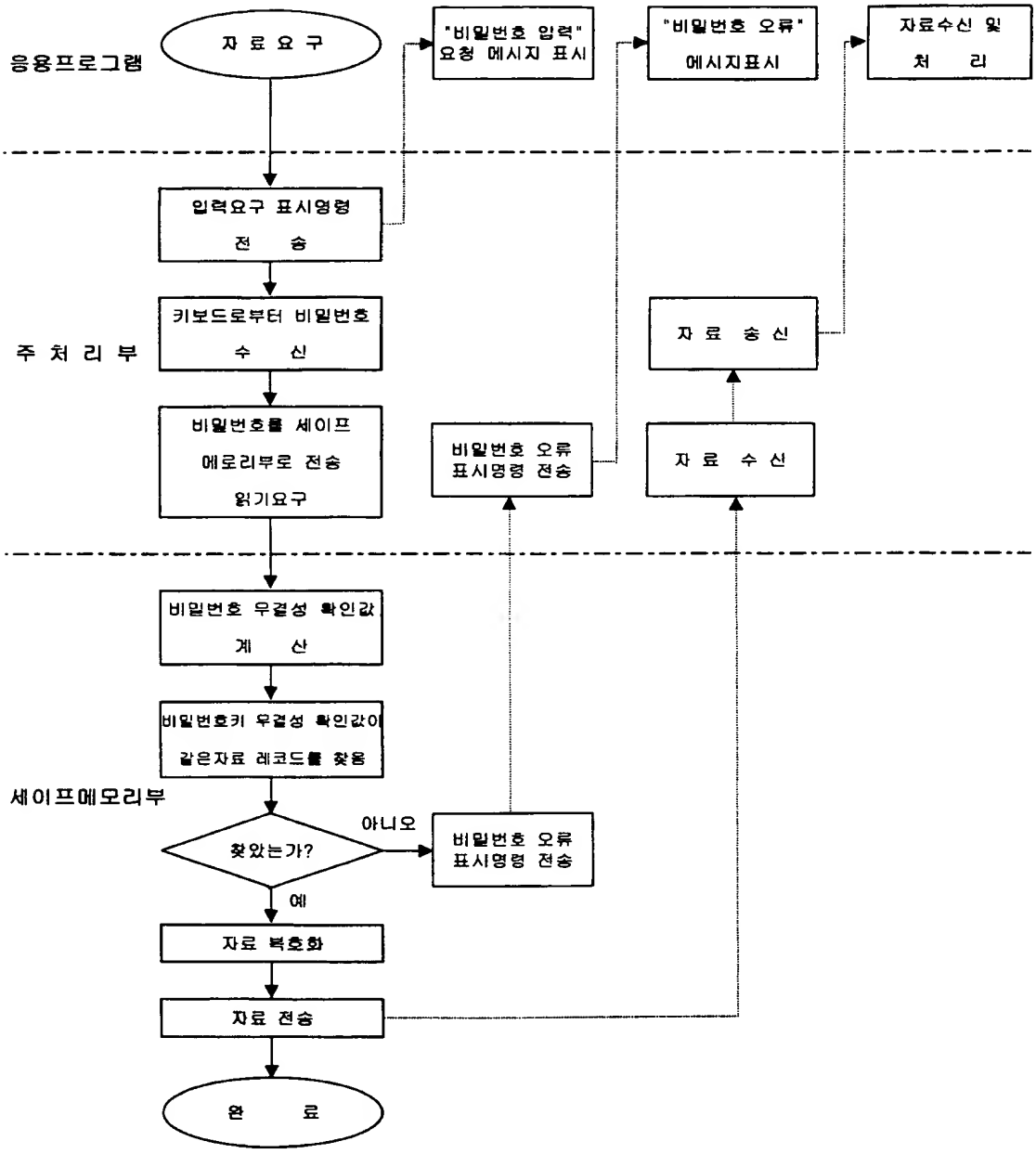
【도 7】


보안모드시 키데이터 처리
키 입 력
비밀키로 암호화
보안 어댑터가 시행
송 신
보안 어댑터가 시행
수 신
키보드 장치관리자가 시행
보관하고 수신한 키 있음을 시스템에 전송
키보드 장치관리자가 시행
응용프로그램이 키데이타를 처리해야 할경우
대 기
입 력 된 키
없다
있다
키보드 장치관리자에게 제일먼저 수신된 키를 복호화 해줄것을 요구
응용프로그램 인터페이스가 시행
장치관리자에서 복호화된 키정보를 받아서 응용프로그램에 전달
응용프로그램 인터페이스가 시행

【도 8】


자 료 입 력
저장된 자료
수신한 자료
응용프로그램
저 장 요 구
"비밀번호 입력" 요청 메시지 표시
"저장중" 메시지표시
표 시 제 거
입력요구 표시명령 전 송
키보드로부터 비밀번호 수 신
주 처 리 부
보안 자료와 비밀번호를 세이프 메모리부로 전송 저장요구
"저장중" 메시지 표시 영령 전송
완료신호 전송
비밀번호키 무결성 확인값 계산
보안자료를 세이프키로 암 호 화
세이프메모리부
암호화된 자료의 무결성 확인값 계산
저 장 (자료, 무결성 확인값)
완료 신호 전송

【도 9】


응용프로그램
자 료 요 구
"비밀번호 입력" 요청 메시지 표시
"비밀번호 오류" 메시지표시
자료수신 및 처 리
입력요구 표시영령 전 송
주 처 리 부
키보드로부터 비밀번호 수 신
자 료 송 신
비밀번호를 세이프 메모리부로 전송 읽기요구
비밀번호 오류 표시명령 전송
자 료 수 신
비밀번호 무결성 확인값 계 산
비밀번호키 무결성 확인값이 같은자료 레코드를 찾음
세이프메모리부
찾았는가?
아니오
비밀번호 오류 표시명령 전송
예
자료 복호화
자료 전송
완 료

【명세서】

【발명의 명칭】

보안기능을 갖는 어댑터 및 이를 이용한 컴퓨터 보안 시스템
{Adapter Having Secure Function and Computer Secure System Using It}

【기술분야】

본 발명은 컴퓨터 시스템과 키보드 사이에 설치하여 사용하는 보안 기능을 가진 어댑터("보안 어댑터") 및 이를 이용한 컴퓨터 보안 시스템에 관한 것으로, 더욱 구체적으로는 보안모드 설정 상태에서는 키보드로부터의 입력정보를 암호화하여 컴퓨터 시스템으로 전달하고 보안모드 해제 상태에서는 상기 입력정보를 암호화하지 않고 컴퓨터 시스템으로 전달하는 구성으로 되어있다.

【배경기술】

컴퓨터의 발전과 인터넷을 통한 정보통신의 비약적 발전은 빠르고 쉽게 정보에 접근할 수 있는 길을 열어 놓았다. 특히, 인터넷은 개인과 기업 업무환경의 정보화와 전자상거래 서비스를 드라이브하는 대표적인 패러다임이며, 그 특성인 개방성(openness)과 표준성(standard)은 그 사용 주체가 개인이든 기업이든 간에 정보교환과 정보공유의 벽을 허물어 버렸다. 반면에, 정보의 보호와 안전한 커뮤니케이션 측면에서 인터넷이 가지고 있는 근본적인 취약점은 커다란 걸림돌로도 작용하고 있다. 따라서, 정보를 다루는 주체들이 서로 신뢰할 수 있는 관계라고 하더라도 인터넷이라는 신뢰할 수 없는 공간을 통해 커뮤니케이션이 이루어지는 한 각각의 서비스 형태나 어플리케이션에 따라 적절한 정보 보호체계가 요구되고 있다.

한편, 컴퓨터를 매개체로한 정보통신의 발달은 인터넷이나 모뎀통신을 사용하여 증권거래, 인터넷 뱅킹, 기타 사이버 거래 등 전자상거래를 가

능하게 한 반면에, 사용자의 정보(자료)가 제3자에 의해 해킹 등과 같은 불법적인 방법에 의해 타인에게 유출되는 경우가 빈번하게 발생하고 있다. 거의 동일한 시스템을 기반으로 한 컴퓨터에 저장된 정보는 해커에 노출되어 있다고 할 수 있다. 따라서, 자신의 컴퓨터에 저장되어 있다고 하여 안전한 정보라고 할 수 없게 되었다. 더욱이, 기술정보, 영업정보 등이 인터넷 등에 의해 전달되고, 전자상거래와 경제활동이 빈번해짐에 따라 개인 정보를 안전하게 보호하는 것이 어느 때보다도 절실하게 되었다.

이와 관련하여, 현재의 컴퓨터는 키보드를 통해 입력된 모든 데이터가 컴퓨터 시스템에 고스란히 전달되어 저장 내지 처리되고 있다. 즉, 현재 사용되고 있는 컴퓨터는 키보드와 컴퓨터 시스템이 직접 연결되어 동작되고 있으므로, 컴퓨터 시스템의 키보드 장치관리자가 키코드값을 키보드 접속 포트에서 받아 컴퓨터 시스템으로 전송하고, 응용 프로그램이 컴퓨터 시스템에서 그 값을 받아 사용하고 있다.

결과적으로, 제3자가 해킹프로그램 등을 통해 키보드 포트에서 상기 값을 수신할 수 있거나 키보드 장치관리자로부터 이 값을 알 수 있다면, 사용자의 비밀자료를 타인이 불법으로 사용할 수 있는 심각한 결과가 초래될 수 있다.

따라서, 본 발명은 이러한 종래 기술의 문제점을 일거에 해결하고 과거로부터 요청되어온 기술적 과제를 해결하는 것을 목적으로 한다.

즉, 키보드를 사용하여 컴퓨터 시스템에 자료를 입력할 때 컴퓨터 시스템과 키보드 사이에 보안관계를 설정할 수 있도록 함으로써, 해킹 등 사용자가 의도하지 않은 방법으로 정보(자료)가 타인에게 유출되는 것을 방지하는 것을 목적으로 한다.

또한, 경우에 따라서는 세이프 메모리부를 부가하여 사용자(User)가

비밀번호를 입력할 때만 자료를 암호화/복호화할 수 있고 암호화에 사용된 비밀번호를 별도로 저장/보관하지 않음으로써, 복제 등의 문제에도 대응할 수 있으며 보안을 요하는 자료의 저장 및 처리가 가능하다.

【발명의 상세한 설명】

이러한 목적을 달성하기 위하여, 본 발명은 키보드로부터의 키코드 입력정보를 컴퓨터 시스템으로 전달하는 보안 어댑터로서, 키보드 또는 컴퓨터 시스템으로부터의 보안모드 설정 명령을 받은 경우에는 키보드로부터의 키코드 입력정보를 암호화하여 컴퓨터 시스템에 전달하고 보안모드 해제 명령을 받거나 보안모드 해제 상태에서는 키보드로부터의 키코드 입력정보를 암호화하지 않고 컴퓨터 시스템으로 전달하는 구성으로 되어있다.

보안모드 설정상태에서 암호화되는 키코드 입력정보는 설정조건에 따라서 모든 키코드일 수도 있고, 특수 키코드를 제외한 문자 및 숫자 키코드만일 수도 있다.

보안모드의 설정 내지 해제는 사용자가 키보드에 별도로 설치한 키("보안키")를 사용하거나 또는 기존 키들의 조합(예컨데, CTRL키+ALT키+SHIFT키+S키)을 사용하여 명령할 수 있다. 또한, 사용자가 키를 사용해 보안모드를 제어하지 않아도 컴퓨터 시스템에서 실행중인 응용프로그램이 상황에 따라 보안모드를 설정 또는 해제할 수도 있다.

보안모드 설정/해제를 위한 구성의 일 예를 보면, 보안 어댑터에는 보안모드 설정/해제 명령을 처리하고 보안모드 설정시 비밀키를 생성하는 주처리부, 주처리부로부터 전송된 비밀키를 컴퓨터 시스템으로부터의 보안키로 암호화하여 컴퓨터 시스템의 키보드 장치관리자로 전송하는 초기 암호화부, 및 키보드로부터의 키코드 입력정보를 비밀키로 암호화하는 스트림 암호화부가 포함되어 있다.

본 발명의 보안 어댑터의 하나의 실시예로서 더욱 구체화된 구성을 도 1을 참고하여 살펴보면,

컴퓨터의 키보드 포트에 연결되는 컴퓨터 연결부;

키보드의 플러그에 연결되는 키보드 연결부;

컴퓨터 시스템과의 통신을 제어하는 컴퓨터측 송수신 제어부;

키보드와의 통신을 제어하는 키보드측 송수신 제어부;

비밀키를 생성하고, 보안모드 관련 명령에 따라 보안모드 설정/해제를 행하며, 컴퓨터 시스템과 키보드의 정보를 상호 전달하는 주처리부;

보안모드가 설정되었을 때, 컴퓨터 시스템으로부터의 보안키로 주처리부로부터의 비밀키를 암호화하여 컴퓨터 시스템으로 전송하는 초기 암호화부; 및

보안모드가 설정되었을 때, 주처리부로부터의 비밀키로 키보드로부터의 키코드 입력정보를 암호화하여 컴퓨터 시스템으로 전송하는 스트림 암호화부를 포함한다.

상기 컴퓨터측 송수신 제어부는 송신할 모든 정보를 입력 버퍼에 우선 기록하고 제어프로그램이 적당한 시기에 이를 전송하며, 수신되는 모든 메시지는 입력 버퍼에 기록되어 다른 모듈에서 사용할 수 있도록 한다.

상기 키보드측 송수신 제어부는 키보드로부터의 키코드 입력정보를 주처리부로 전송하고, 전송될 모든 명령이 버퍼에 기록되며 본 모듈이 적당한 시기에 전송하게 된다.

상기 스트림 암호화부(stream cipher)는 주처리부로부터 전송된 정보를 비밀키로서 암호화하는데, 스트림 암호는 모든 평문에 동일한 암호화 함수가 적용되어지는 블록 암호와는 달리 평문의 비트 또는 문자가 암호화되어짐에 따라서 상이한 암호화 함수가 적용되고 각각의 평문 비트가 다른

비트와는 관계없이 암호화되기 때문에 암호화의 속도가 비교적 빠르며, 암호화 과정이나 전달과정에서 특정 비트에 발생되는 채널오류(channel error)의 영향이 해당 비트에만 적용될 뿐 다른 비트들에는 파급(propagation)이 되지 않는 장점이 있다. 그러나, 필요에 따라서는 스트림 암호가 아닌 블록 암호를 사용한 구성을 사용할 수도 있다.

상기 컴퓨터 연결부와 키보드 연결부는 통상 5V의 전원을 공급받고 통신선으로 연결된다. 그러나, 본 발명의 보안 어댑터는 반드시 키보드 및 컴퓨터 시스템과 외형상으로 분리된 장치일 필요는 없고, 컴퓨터 본체 또는 키보드에 함께 체결된 구조일 수 있다. 이 경우, 컴퓨터 본체와 키보드의 송수신 수단은 반드시 케이블일 필요는 없는바, 예를 들어 키보드에는 무선 정보 송신부가 설치되어 있고 컴퓨터 본체에는 무선 정보 수신부가 설치되어 있는 구조일 수 있다. 도 2에는 컴퓨터 시스템과 키보드 사이에 독립적 장치로서 연결되어 있는 보안 어댑터의 예가 도시되어 있다. 보안 어댑터에는 동작상태 표시램프와 보안모드 표시램프(후술함)가 설치되어있다.

본 발명의 보안 어댑터에는 하나 또는 둘 이상의 표시램프를 둘 수 있다. 그러한 표시 램프는 보안 어댑터의 작동을 표시하는 동작상태 표시램프, 보안상태를 표시하는 보안모드 표시램프 등이 있다. 이 경우, 보안모드 표시램프는 주처리부에서 제어되는데, 보안모드 설정 상태에서는 모안모드 표시램프가 점등되고, 보안모드 해제 상태에서는 모안모드 표시램프가 소등되며, 보안모드 불능 상태에서는 모안모드 표시램프가 주기적으로 깜박이게 된다. 상기 보안모드 불능 상태란 컴퓨터 시스템, 보안키 및/또는 비밀키의 설정이 제대로 이루어지지 않은 상태를 의미한다. 이러한 보안모드 표시램프는 반드시 보안 어댑터에만 설치하여야 하는 것은 아니고, 경우에 따라서는 컴퓨터 본체 전면, 키보드 또는 모니터 상에 설치할 수 있다. 경

우에 따라서는 보안모드 설정 여부를 모니터상의 설정 화면내에 작은 표시부(예를 들어, 아이콘 형태 등)로 둘 수도 있다.

경우에 따라서는, 상기 보안 어댑터의 주요 구성에 연동되는 세이프 메모리부를 부가할 수 있다. 상기 세이프 메모리부는 컴퓨터 시스템에서 실행되는 응용프로그램이 필요에 따라 설정한 보안모드하에서 작동되며, 별도의 보안을 필요로하는 암호화 자료의 저장 및 처리에 사용된다.

더욱 구체적으로, 상기 세이프 메모리부는,

주처리부로부터 전송된 비밀번호, 또는 비밀번호와 보안을 요하는 자료("보안 자료")를 암호화/키연산 프로세서로 전송하고 복호화부로부터 수신한 자료를 주처리부로 전송하는 세이프 메모리 인터페이스;

세이프 메모리 인터페이스로부터 수신한 비밀번호를 키("세이프키")로 전환한 뒤 보안 자료가 함께 수신되지 않았으면 상기 세이프키를 복호화부로 전송하고, 암호화 알고리즘에 의해 상기 세이프키로 비밀번호를 암호화하여 그것의 무결성 확인값("비밀번호 무결성 확인값")을 계산한 뒤 비교/처리부로 전송하며, 세이프 메모리 인터페이스로부터 수신한 보안 자료가 있으면 이를 상기 세이프키로 암호화하고 그것의 무결성 확인값("암호화 자료 무결성 확인값")을 계산하여 "암호화 자료"와 함께 비교/처리부로 전송하는 암호화/키연산 프로세서;

암호화/키연산 프로세서로부터 수신된 "비밀번호 무결성 확인값"과 자료저장 메모리에 저장된 "비밀번호 무결성 확인값"을 비교하여, 상호 무결성 확인값이 동일하면 저장된 자료들을 복호화부로 전송하고, 상호 무결성 확인값이 동일하지 않으면 비밀번호 불일치 사실을 컴퓨터 시스템에 전송하고 복호화부에 임시 저장된 세이프키를 삭제하며, "비밀번호 무결성 확인값"과 함께 "암호화 자료" 및 "암호화 자료 무결성 확인값"이 암호화/키연

산 프로세서로부터 함께 수신된 경우에는 이들 자료를 자료저장 메모리로 전송하는 비교/처리부;

암호화 자료, 암호화 자료 무결성 확인값 및 비밀번호 무결성 확인값을 저장하는 자료 저장 메모리; 및

자료저장 메모리로부터의 암호화 자료를 세이프키로 복호화하여 세이프 메모리 인터페이스로 전송하는 복호화부를 포함하고 있다.

이때, 보안 어댑터의 주처리부는, 컴퓨터 시스템의 응용프로그램으로부터 수신된 보안모드 설정 명령이 세이프 메모리에 관한 것일 때 비밀번호 입력 요청 명령을 컴퓨터 시스템으로 전송하며, 키보드로부터 수신한 비밀번호를 세이프 메모리부로 전송하는 기능을 부가적으로 갖는다.

상기 세이프 메모리부는 별도로 비밀번호를 저장하지는 않고, 암호화 자료의 저장시 사용된 비밀번호와 동일한 비밀번호를 사용자(User)가 입력한 경우에만 비밀번호로부터 전환된 세이프키를 사용하여 복호화 작업을 실행하게 된다. 올바른 비밀번호가 입력되었는지 여부는 자료저장 메모리의 암호화 자료와 함께 저장되어 있는 "비밀번호 무결성 확인값"을, 새로 입력된 비밀번호로 전환된 세이프키로 암호화된 후에 계산된 "비밀번호 무결성 확인값"과 비교하여, 동일한 경우에 유효한 접속으로 인정하게 된다.

따라서, 암호화/키연산 프로세서로부터 복호화부로 전송된 세이프키는 복호화부의 버퍼에 임시 저장되어 있다가, 비교/처리부의 실행 결과, 저장되어 있는 "비밀번호 무결성 확인값"과 새로 입력된 비밀번호로부터 계산된 "비밀번호 무결성 확인값"이 동일하지 않을 경우에는, 비교/처리부의 명령에 따라 상기 세이프키가 버퍼에서 삭제된다.

상기 비밀번호의 세이프키로의 변환은 공지되어 있는 해쉬 함수 또는 다항식 등 공지의 다양한 알고리즘에서 선택하여 사용할 수 있다. 그러

한 대표적인 예로는 MAC 해쉬함수, MDC 해쉬함수, MD4 해쉬함수, MD5 해쉬함수, SHA 해쉬함수, CRC 알고리즘 등이 있다.

상기 무결성 확인(Integrity Identification)은 접속자의 실체 확인을 위한 수단으로 사용됨으로써 해커의 능동적인 공격에 대해 자료를 보호하게 된다. 그러한 무결성을 확인하기 위한 방법으로는, 상기에서와 같은 공지의 다양한 알고리즘을 선택하여 사용할 수 있으며, 그 중에서도 CRC(Cyclic Redundancy Checking: 순환 중복 검사) 알고리즘이 특히 바람직하다. CRC 알고리즘은 K개의 비트로 구성된 데이터를 전송할 때, 전송할 데이터를 n+1 개의 비트 패턴으로 나누어 이때 발생한 n 비트 길이의 나머지를 데이터 비트 뒷부분에 붙여 모두 k+n 개의 비트로 구성된 데이터를 전송한다. 그리고, 데이터를 수신하는 곳에서는 다시 n 개의 비트로 구성되어 패턴으로 수신 데이터를 나누어 이때 발생하는 나머지 값을 통해 데이터 전송 오류를 발견하는 구성의 알고리즘으로서, 데이터를 수신한 곳에서 나머지가 0이면 데이터 전송에 오류가 없는 것이고, 나머지가 1이면 데이터 전송에 오류가 발생한 것이 된다. 따라서, 본 발명에서는 비밀번호로부터 전환된 세이프키로 암호화된 자료의 CRC 값("암호화 자료 CRC 값")과 비밀번호의 CRC 값("비밀번호 CRC 값")을 계산하여 자료저장 메모리에 저장하고, 컴퓨터 시스템의 응용프로그램이 보안상태의 자료를 획득하고자 할 때 사용자가 입력한 비밀번호로부터 계산된 "비밀번호 CRC 값"을 자료저장 메모리에 저장되어 있는 "비밀번호 CRC 값"과 비교하는 방식으로, 통신상의 데이터 전송 오류발생여부 확인 알고리즘의 구성이 변형되어 사용된다. 따라서, 저장된 CRC 값과 새로 계산된 CRC 값이 동일한 경우에는, 자료 저장시 사용된 비밀번호와 동일한 비밀번호를 입력한 사용자가 컴퓨터 시스템을 접속하고 있음을 확인하게 된다. 상기에서 n은 16 또는 32 비트인바, 본 발

명에서는 바람직하게는 16 비트를 사용한다.

상기 세이프키를 암호화하는데 사용되는 암호화 알고리즘은 공지되어 있는 다양한 암호화 알고리즘에서 선택하거나 별도로 제작하여 사용할 수 있다.

자료저장 메모리에는 "비밀번호 무결성 확인값"과 "암호화 자료 무결성 확인값"이 함께 저장되는데, 상기 "비밀번호 무결성 확인값"이 자료를 새로 입력한 비밀번호가 올바른지를 확인하기 위하여 사용되는 반면에, 상기 "암호화 자료 무결성 확인값"은 암호화된 자료가 오류없이 저장되었는지 또는 저장중 오류가 발생하였는지를 확인하는 목적으로 사용될 수 있다. 즉, 복호화된 자료를 세이프키로 재차 암호화하고 암호화된 자료의 무결성 확인값을 계산하여 자료저장 메모리에 수록되어 있던 암호화 자료 무결성 확인값과 비교함으로써 이를 확인할 수 있다. 따라서, 이러한 기능을 실행할 수 있는 별도의 모듈을 부가하거나 상기 기본 구성 모듈에 이러한 기능을 첨가하여, 상기 암호화 자료의 저장중 또는 복호화 과정중에 오류가 발생했는지 여부를 확인할 수 있다.

한편, 다수의 암호화 자료를 한번에 또는 여러 차례에 걸쳐 자료저장 메모리에 저장할 때 각각 다른 비밀번호를 사용하게 되면, 암호화 자료에 대해 다른 "비밀번호 무결성 확인값"이 저장되게 된다. 다시 말하면, 자료를 저장할 때 비밀번호를 다르게 설정하여 암호화 자료의 종류를 특정할 수도 있다. 따라서, 필요에 따라서는 자료저장 메모리에 저장되어 있는 암호화 자료의 비밀번호 무결성 확인값을 암호화 자료의 종류에 따라 다르게 설정할 수도 있다. 암호화 자료의 인출과정에서는 같은 "비밀번호 무결성 확인값"이 설정되어 있는 암호화 자료가 함께 복호화된다.

상기 세이프 메모리부에서 사용되는 암호화 알고리즘은 상기 보안

어댑터의 스트림 암호화부에서 사용되는 암호화 알고리즘과 서로 다를 수 있다.

본 발명은 또한 상기 보안 어댑터와 키보드 및 컴퓨터 시스템으로 구성되어 있는 컴퓨터 보안 시스템에 관한 것이다.

키보드에는 보안모드 설정/해제의 명령을 입력하기 위한 별도의 보안키가 설치되어 있거나 및/또는 기존 키코드의 조합에 의해 보안모드 설정/해제의 명령이 생성된다. 컴퓨터 시스템에는 보안키를 생성하는 기능, 비밀키로 암호화/복호화하는 기능, 보안키로 암호화/복호화하는 기능을 가지며, 응용프로그램 인터페이스가 있는 키보드 장치관리자가 포함되어있다. 응용프로그램 인터페이스는 컴퓨터 시스템의 응용프로그램에서 직접 복호화할 수 있는 기능을 가지거나 및/또는 컴퓨터 시스템의 운영체제가 복호화할 수 있도록 하는 기능을 제공한다.

컴퓨터 시스템의 키보드 장치관리자에서 생성된 보안키는 보안모드 설정시 보안 어댑터로 전송되고, 보안 어댑터로 전송된 보안키는 보안모드 설정시마다 어댑터로부터 새로이 생성된 비밀키를 암호화하여 컴퓨터 시스템으로 재전송하면, 이후 키보드로부터 입력된 키코드값을 보안 어댑터에서 받아 비밀키로 암호화하여 컴퓨터 시스템에 전송하게 되고, 컴퓨터 시스템은 보안 어댑터로부터 전송받은 암호화된 키코드 입력정보를 보관중인 비밀키로 복호화하여 처리하게 된다.

컴퓨터 시스템에는 상기 키보드 장치관리자 이외에 일반적인 운영체제, 응용프로그램 등이 있으며, 암호화된 정보를 복호화하는 기능은 상기 키보드 장치관리자, 운용체계 및/또는 응용프로그램 등에서 가질 수 있다. 여기서, 응용프로그램과 키보드 장치관리자간 및 운용체계와 키보드 장치관리자간에는 복호화된 정보를 획득하기 위한 프로토콜이 있는데, 이는 제 3

자가 키보드 장치관리자의 외부인터페이스를 임의로 도용하여 해킹하는 프로그램의 작성을 방지하기 위함이다.

윈도우 98(마이크로소프트사 제품) 환경하에서 실행될 수 있고 키보드 장치관리자가 복호화 기능을 가진 컴퓨터 시스템의 일 예를 도 3을 참조하여 설명하면 하기와 같다. 다만, 윈도우 98 환경이외에 윈도우 2000, 윈도우/NT, 유닉스, 리눅스 등과 같이 프로토콜이 다른 환경 하에서도 하기 내용을 바탕으로 적절한 프로토콜을 적용할 수 있다.

컴퓨터 시스템이 작동되면, 키보드 장치관리자는 보안키를 만들어 보안 어댑터로 보내고, 보안모드시 보안키로 암호화된 비밀키를 보안 어댑터로부터 수령하며, 이후에는 비밀키로 암호화된 키코드 입력정보를 보안 어댑터로부터 수령하게 된다. 키보드 장치관리자가 보안 어댑터로부터 수령한 암호화 키코드 입력정보는 곧바로 복호화되는 것은 아니고 키보드 장치관리자내에 또는 컴퓨터 시스템의 기타 장소에 저장되며, 운영체제를 통해 어떠한 키코드가 눌려졌다는 신호만을 응용프로그램 인터페이스에 보낸다.

한편, 응용프로그램이 작동하다가 전달된 키코드를 조사하려하면, 응용프로그램 인터페이스가 이를 가로채어 키보드 장치관리자에게 제일 먼저 눌려진 키코드를 복호화해줄 것을 키보드 장치관리자에게 요청하게 되고, 키보드 장치관리자는 저장해둔 암호화 키코드 입력정보를 보관중인 비밀키로 복호화하여 응용프로그램 인터페이스에 전달하게 되며, 응용프로그램 인터페이스는 복호화된 키코드 입력정보를 조사결과로서 응용프로그램에 돌려주게 된다.

참고로, 본 발명에서의 컴퓨터 시스템의 부팅 과정을 보면, 전원의 인가시, BIOS 동작, LOADER 동작, KERNEL 동작, 키보드 장치관리자 동작,

O.S 동작 순으로 진행되므로, 키보드 장치관리자는 초기 전원의 인가 후 운영체제(O.S)가 로딩되는 중에 실행되므로 일반 해킹프로그램이나 응용프로그램보다 먼저 실행된다.

한편, 모안모드 해제시에는 키보드 장치관리자로 전달된 암호화되지 않은 키보드 입력정보가 운용체제를 거쳐 응용프로그램에 직접 전달되게 된다.

본 발명의 보안 어댑터의 주요 구성에 세이프 메모리부가 부가된 경우의 예를 도 4를 참고로 설명하면 다음과 같다. 본 실시예에서는 무결성 확인값을 CRC 알고리즘을 사용하여 계산한 경우로 특정하였다.

컴퓨터 시스템의 응용프로그램으로부터 보안모드 설정 명령과 함께 보안을 요하는 자료의 저장 내지 처리 명령이 주처리부로 전송되면, 주처리부는 시스템을 보안모드로 전환하고, 비밀번호의 입력 요청 명령을 컴퓨터 시스템으로 전송한다. 컴퓨터 시스템이 비밀번호 입력 요청을 모니터상에 띄우면 사용자가 비밀번호를 입력하게 되고, 비밀번호 입력 내용이 키보드 송수신 제어부를 통해 주처리부로 전송되고 주처리부는 일를 세이프 메모리부의 인터페이스로 전송한다.

응용프로그램으로부터의 보안모드 설정 명령이 보안을 요하는 자료의 저장에 관한 것이면, 응용프로그램으로부터 자료가 주처리부로 전송되고 주처리부는 이를 받아 세이프 메모리부의 인터페이스로 전송한다. 세이프 메모리 인터페이스는 비밀번호와 보안 자료를 암호화/키연산 프로세서로 전송하면, 암호화/키연산 프로세서는 비밀번호를 세이프키로 전환하고 세이프키를 이용하여 보안 자료와 비밀번호를 암호화한다. 한편, 암호화/키연산 프로세서는 암호화 비밀번호와 암호화 자료의 CRC 값을 계산하여, "암호화 자료", "비밀번호 CRC 값" 및 "암호화 자료 CRC 값"을 비교/처리부로 전송

한다. 비교/처리부는 이들 정보를 자료저장 메모리에 저장한다.(도 8 참조)

한편, 응용프로그램으로부터의 보안모드 설정 명령이, 저장된 암호화 정보의 복호화에 관한 것이면, 세이프 메모리 인터페이스로 전송된 비밀번호만을 암호화/키연산 프로세서로 전송하고, 암호화/키연산 프로세서는 비밀번호를 세이프키로 전환한 다음 세이프키로 비밀번호를 암호화하여 암호화된 비밀번호의 CRC 값("비밀번호 CRC 값")을 계산하며, "세이프키"는 복호화부로 전송하고 "비밀번호 CRC 값"은 비교/처리부로 각각 전송한다. 비교/처리부는 자료저장 메모리를 스캐닝하여 메모리에 저장되어 있는 "비밀번호 CRC 값"이 암호화/키연산 프로세서로부터 수신한 "비밀번호 CRC 값"과 동일한지 여부를 확인한다. 상호 CRC 값이 동일한 경우에는 자료저장 메모리로부터 암호화 자료를 수신하여 복화부로 전송하고, 복호화부는 비교/처리부로부터 수신한 암호화 자료를 세이프키로 복호화하여 세이프 메모리 인터페이스로 전송한 후 세이프키를 삭제한다. 상호 CRC 값이 동일하지 않은 경우에는 비교/처리부는 복호화부의 버퍼에 저장되어 있는 세이프키를 삭제하고 비밀번호의 불일치 사실을 컴퓨터 시스템으로 전송한다.(도 9 참조)

복호화된 자료가 다시 스트림 암호화부에서 비밀키로 암호화되어 컴퓨터 시스템으로 전송되는 과정은 보안 어댑터의 주요 구성에 대한 앞서의 설명과 같다. 그러나, 경우에 따라서는 세이프 메모리부로부터 복호화되어 전송된 자료는 스트림 암호화부에서 재차 암호화되지 않은 상태에서 컴퓨터 시스템으로 전송되도록 구성할 수도 있다.

본 발명은 또한 컴퓨터 보안 시스템을 이용하여 키보드로부터 전송되는 키코드 입력정보를 보안화하는 방법에 관한 것이다.

구체적으로는, 컴퓨터 부팅시 컴퓨터 시스템의 키보드 장치관리자에

서 생성된 보안키가 보안 어댑터로 전송되는 단계;

키보드 또는 컴퓨터 시스템으로부터 보안모드 설정 명령이 보안 어댑터의 주처리부로 전송되었을 때, 주처리부에서 새로 비밀키를 생성하여 보안 어댑터의 초기 암호화부 및 스트림 암호화부로 전송하는 단계;

초기 암호화부에서 보안키로 비밀키를 암호화하여 컴퓨터측 송수신 제어부를 통해 컴퓨터 연결부를 거쳐 키보드 장치관리자로 전송하는 단계;

보안모드 설정하에서, 키보드의 키코드 입력정보가 키보드측 송수신 제어부를 거쳐 주처리부로 전송되면, 주처리부는 이를 스트림 암호화부로 전송하며, 스트림 암호화부는 키코드 입력정보를 비밀키로 암호화하여 컴퓨터측 송수신 제어부를 통해 컴퓨터 연결부를 거쳐 키보드 장치관리자로 전송하는 단계;

컴퓨터 시스템은 암호화된 정보를 비밀키를 이용하여 복호화하는 단계;

키보드 또는 컴퓨터 시스템으로부터 보안모드 해제 명령이 보안 어댑터의 주처리부로 전송되었을 때, 주처리부에서 보안모드 해제 명령을 스트림 암호화부로 전송하는 단계;

보안모드 해제하에서, 키보드의 키코드 입력정보가 키보드 연결부를 거쳐 키보드측 송수신 제어부를 통해 스트림 암호화부로 전송되면, 스트림 암호화부는 전송된 키코드 입력정보를 암호화하지 않고 컴퓨터측 송수신 제어부를 통해 컴퓨터 연결부를 거쳐 키보드 장치관리자로 전송하는 단계를 포함한다.

보안 어댑터의 주요 구성에 세이프 메모리부를 부가한 경우에는,

보안모드 설정이 컴퓨터 시스템의 응용프로그램으로부터의 명령에 의한 것이면서 동시에 보안을 요하는 자료의 저장에 관한 것일 때, 주처리

부가 비밀번호의 입력 요청 명령을 컴퓨터 시스템에 전송한 후, 키보드측 송수신 제어부로부터 수신한 비밀번호와 컴퓨터측 송수신 제어부로부터 수신한 보안 자료를 세이프 메모리부로 전송하며, 세이프 메모리는 수신한 자료를 비밀번호를 이용하여 암호화한 후 저장하고,

반면에 보안모드 설정이 컴퓨터 시스템의 응용프로그램으로부터의 명령에 의한 것이면서 동시에 보안 자료의 획득에 관한 것일 때, 주처리부는 비밀번호의 입력 요청 명령을 컴퓨터 시스템에 전송한 후, 키보드측 송수신 제어부로부터 수신한 비밀번호를 세이프 메모리부로 전송하며, 비밀번호가 올바른 경우 세이프 메모리부는 암호화된 자료를 비밀번호를 이용하여 복호화한 후에 주처리부로 전송하고, 비밀번호가 올바르지 않을 경우 세이프 메모리부는 암호화된 자료를 복호화하지 않는 단계를 더 포함한다.

본 발명의 컴퓨터 보안 시스템에 의한 보안모드 설정/해제시 보안 어댑터에서의 작동 과정을 도 1을 바탕으로 설명하면 다음과 같다.

컴퓨터가 부팅(전원이 넣어져서 오퍼레이팅 시스템이 실행되어 사용 가능한 상태로 되는 작업)되면, 컴퓨터 시스템(도시하지 않음)의 키보드 장치관리자는 보안키를 컴퓨터 연결부를 거쳐 컴퓨터측 송수신 제어부를 통해 주처리부로 전송한다. 주처리부는 동작상태 표시램프를 점등(ON)하고 보안키를 초기 암호화부로 전송한다.

한편, 키보드로부터의 키코드 입력정보는 키보드 연결부를 통해 키보드측 송수신 제어부를 거쳐 주처리부로 전송된다. 주처리부는 키보드로부터 전송된 입력정보가 보안모드 설정에 관한 것이면, 보안모드 표시램프를 점등(ON)하고 비밀키를 생성하여 초기 암호화부와 스트림 암호화부로 전송하고, 키코드 입력정보를 또한 스트림 암호화부로 전송한다. 초기 암호화부는 보안키로 비밀키를 암호화하여 컴퓨터측 송수신 제어부를 통해

컴퓨터 연결부를 거쳐 컴퓨터 시스템의 키보드 장치관리자로 전송한다. 한편, 스트림 암호화부는 주처리부로부터 전송된 비밀키를 사용하여 키코드 입력정보를 암호화한 후 컴퓨터측 송수신 제어부를 통해 컴퓨터 연결부를 거쳐 컴퓨터 시스템의 키보드 장치관리자로 전송하게 된다. 키보드 장치관리자로 전송된 암호화된 키코드 입력정보의 컴퓨터 시스템내에서의 처리과정은 도 3을 바탕으로 앞서 설명한 내용을 참조하면 된다.

컴퓨터 시스템이나 키보드로부터 보안모드 해제 명령이 오면, 상기 해제 명령은 컴퓨터측 송수신 제어부나 키보드측 송수신 제어부를 거쳐 주처리부와 스트림 암호화부로 전달된다. 주처리부는 보안모드 표시램프를 소등(OFF)하고 스트림 암호화부에 보안모드 해제 명령을 전송한다. 이후 키보드로부터 전송된 키코드값은 스트림 암호화부에서 암호화되지 않고 컴퓨터측 송수신 제어부를 통해 컴퓨터 연결부를 거쳐 컴퓨터 시스템에 전송된다. 키보드 장치관리자로 전송된 암호화되지 않은 키코드 입력정보의 컴퓨터 시스템내에서의 처리 과정은 도 3을 바탕으로 앞서 설명한 내용을 참조하면 된다.

컴퓨터의 부팅시 컴퓨터 시스템의 키보드 장치관리자로부터 보안키를 받지 못한 경우에는 보안 어댑터가 보안모드 불능상태가 되고 주처리부는 보안모드 표시램프에 주기적인 점등 및 소등 신호를 전송하게 된다. 이때, 키보드 장치관리자 및 복호화된 자료전달 프로토콜에 의하여 보안모드 불능상태가 모니터상에 메시지의 형태 등으로서 고지될 수 있고, 키보드 입력정보는 암호화되지 않은 상태로 키보드 장치관리자에게 전달된다.

도 5 내지 도 7에는 본 발명에서 보안모드 설정과정과, 보안모드 해제과정 및 보안모드 설정하에서의 키코드 입력정보의 처리과정이 더욱 자세히 도시되어 있다.

도 8에는 세이프 메모리부가 부가된 보안 어댑터에서 자료를 암호화하여 저장 과정이 도시되어 있고, 도 9에는 암호화된 자료를 복호화하는 과정이 도시되어 있다.

본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이상의 내용을 바탕으로 본 발명의 범주내에서 다양한 변경 및 응용이 가능할 것이다.

【도면의 간단한 설명】

도 1은 본 발명 보안 어댑터의 하나의 실시예로서 모듈의 구성도이고;

도 2는 컴퓨터 시스템과 키보드 사이에 케이블로 연결된 본 발명 보안 어댑터의 하나의 실시예에 대한 사시도이고;

도 3은 본 발명 컴퓨터 보안 시스템 중 컴퓨터 시스템의 개략적 구성도이고;

도 4는 도 1의 보안 어댑터에 세이프 메모리부가 부가된 모듈의 구성도이고;

도 5는 본 발명에서 보안모드 설정시의 과정 단계도이고;

도 6은 본 발명에서 해제모드 설정시의 과정 단계도이고;

도 7은 본 발명에서 보안모드시의 키코드 입력정보의 처리과정 단계도;

도 8은 도 4의 보안 어댑터에서 자료를 암호화하여 저장하는 과정에 대한 단계도이고;

도 9는 도 4의 보안 어댑터에서 저장된 암호화 자료를 복호화하는 과정의 단계도이다.

【산업상이용가능성】

본 발명의 보안 어댑터 및 이를 포함한 컴퓨터 보안 시스템을 사용

하면, 인터넷이나 모뎀통신 등과 데이터 네트워크상에서 사용하여 증권거래, 인터넷 뱅킹, 사이버 거래 등을 함에 있어서, 제 3자가 해킹 등의 방법으로 컴퓨터 시스템에 침입하여 사용자의 비밀자료를 도용하는 것을 막을 수 있다.

【청구의 범위】

【청구항 1】

키보드로부터의 키코드 입력을 컴퓨터 시스템으로 전달하는 어댑터로서, 키보드 또는 컴퓨터 시스템으로부터의 보안모드 설정 명령을 받은 경우에는 키보드로부터의 입력을 암호화하여 컴퓨터 시스템에 전달하고 보안모드 해제 명령을 받거나 보안모드 해제 상태에서는 키보드로부터의 입력을 암호화하지 않고 컴퓨터 시스템으로 전달하는 구성으로 되어 있는 것을 특징으로 하는 보안 어댑터.

【청구항 2】

제 1항에 있어서, 보안모드 설정/해제 명령을 처리하고 보안모드 설정시 비밀키를 생성하는 주처리부, 주처리부로부터 전송된 비밀키를 보안키로 암호화하여 컴퓨터 시스템으로 전송하는 초기 암호화부, 및 키코드 입력 정보를 비밀키로 암호화하여 컴퓨터 시스템으로 전송하는 스트림 암호화부를 포함하는 것을 특징으로 하는 보안 어댑터.

【청구항 3】

제 1항에 있어서, 컴퓨터의 키보드 포트에 연결되는 컴퓨터 연결부; 키보드의 플러그에 연결되는 키보드 연결부; 컴퓨터 시스템과의 통신을 제어하는 컴퓨터측 송수신 제어부; 키보드와의 통신을 제어하는 키보드측 송수신 제어부; 비밀키를 생성하고, 보안모드 관련 명령에 따라 보안모드 설정/해제를 행하며, 컴퓨터 시스템과 키보드의 정보를 상호 전달하는 주처리부; 보안모드가 설정되었을 때, 컴퓨터 시스템으로부터의 보안키로 주처리부로부터의 비밀키를 암호화하여 컴퓨터 시스템으로 전송하는 초기 암호화부; 및 보안모드가 설정되었을 때, 주처리부로부터의 비밀키로 키코드 입력 정보를 암호화하여 컴퓨터 시스템으로 전송하는 스트림 암호화부를 포함하

는 것을 특징으로 하는 보안 어댑터.

【청구항 4】

제 1항에 있어서, 보안모드 설정 상태에서는 램프가 점등되고, 보안모드 해제 상태에서는 램프가 소등되며, 보안모드 불능 상태에서는 램프가 주기적으로 깜박이는 보안모드 표시램프가 부설되어 있는 것을 특징으로 하는 보안 어댑터.

【청구항 5】

제 1항 내지 제 4항 중 어느 하나에 있어서,

컴퓨터 시스템에서 실행되는 응용프로그램이 필요에 따라 설정한 보안모드하에서 작동되는 세이프 메모리부가 부가되어 있으며, 상기 세이프 메모리부는,

주처리부로부터 전송된 비밀번호, 또는 비밀번호와 보안을 요하는 자료("보안 자료")를 암호화/키연산 프로세서로 전송하고 복호화부로부터 수신한 자료를 주처리부로 전송하는 세이프 메모리 인터페이스;

세이프 메모리 인터페이스로부터 수신한 비밀번호를 키("세이프키")로 전환한 뒤 보안 자료가 함께 수신되지 않았으면 상기 세이프키를 복호화부로 전송하고, 암호화 알고리즘에 의해 상기 세이프키로 비밀번호를 암호화하여 그것의 무결성 확인값("비밀번호 무결성 확인값")을 계산한 뒤 비교/처리부로 전송하며, 세이프 메모리 인터페이스로부터 수신한 보안 자료가 있으면 이를 상기 세이프키로 암호화하고 그것의 무결성 확인값("암호화 자료 무결성 확인값")을 계산하여 암호화 자료와 함께 비교/처리부로 전송하는 암호화/키연산 프로세서;

암호화/키연산 프로세서로부터 수신된 "비밀번호 무결성 확인값"과 자료저장 메모리에 저장된 "비밀번호 무결성 확인값"을 비교하여, 상호 무

결성 확인값이 동일하면 저장된 자료들을 복호화부로 전송하고, 상호 무결성 확인값이 동일하지 않으면 비밀번호 불일치 사실을 컴퓨터 시스템으로 전송하고 복호화부에 임시 저장된 세이프키를 삭제하며, "비밀번호 무결성 확인값"과 함께 "암호화 자료" 및 "암호화 자료 무결성 확인값"이 암호화/키 연산 프로세서로부터 함께 수신된 경우에는 이들 자료를 자료저장 메모리로 전송하는 비교/처리부;

암호화 자료, 암호화 자료 무결성 확인값 및 비밀번호 무결성 확인값을 저장하는 자료 저장 메모리; 및

자료저장 메모리로부터의 암호화 자료를 세이프키로 복호화하여 세이프 메모리 인터페이스로 전송하는 복호화부를 포함하고 있고,

상기 세이프 메모리부가 부가되어 있을 때, 주처리부는 컴퓨터 시스템의 응용프로그램으로부터 수신된 보안모드 설정 명령이 세이프 메모리에 관한 것일 때는 비밀번호 입력 요청 명령을 컴퓨터 시스템으로 전송하며, 키보드로부터 수신한 비밀번호를 세이프 메모리부로 전송하는 기능을 부가적으로 갖는 것을 특징으로 하는 보안 어댑터.

【청구항 6】

제 5항에 있어서, 상기 무결성 확인값이 CRC 알고리즘에 의해 계산된 값인 것을 특징으로 하는 보안 어댑터.

【청구항 7】

제 1항 내지 제 6항의 보안 어댑터와 키보드 및 컴퓨터 시스템으로 구성되어 있고, 상기 키보드에는 보안모드 설정/해제의 명령을 입력하기 위한 별도의 보안키가 설치되어 있거나 및/또는 기존 키코드의 조합에 의해 보안모드 설정/해제의 명령을 생성할 수 있으며, 상기 컴퓨터 시스템에는 보안키를 생성하는 기능, 비밀키로 암호화/복호화하는 기능, 보안키로 암호

화/복호화하는 기능을 가지며, 응용프로그램 인터페이스가 있는 키보드 장치관리자가 포함되어 있는 것을 특징으로 하는 컴퓨터 보안 시스템.

【청구항 8】

컴퓨터 부팅시 컴퓨터 시스템의 키보드 장치관리자에서 생성된 보안키가 보안 어댑터로 전송되는 단계;

키보드 또는 컴퓨터 시스템으로부터 보안모드 설정 명령이 보안 어댑터의 주처리부로 전송되었을 때, 주처리부에서 새로 비밀키를 생성하여 보안 어댑터의 초기 암호화부 및 스트림 암호화부로 전송하는 단계;

초기 암호화부에서 보안키로 비밀키를 암호화하여 컴퓨터측 송수신 제어부를 통해 컴퓨터 연결부를 거쳐 키보드 장치관리자로 전송하는 단계;

보안모드 설정하에서, 키보드의 키코드 입력정보가 키보드측 송수신 제어부를 거쳐 주처리부를 통해 스트림 암호화부로 전송되면, 스트림 암호화부는 키코드 입력정보를 비밀키로 암호화하여 컴퓨터측 송수신 제어부를 통해 컴퓨터 연결부를 거쳐 키보드 장치관리자로 전송하는 단계;

컴퓨터 시스템은 암호화된 정보를 비밀키를 이용하여 복호화하는 단계;

키보드 또는 컴퓨터 시스템으로부터 보안모드 해제 명령이 보안 어댑터의 주처리부로 전송되었을 때, 주처리부에서 보안모드 해제 명령을 스트림 암호화부로 전송하는 단계;

보안모드 해제하에서, 키보드의 키코드 입력정보가 키보드측 송수신 제어부를 거쳐 주처리부를 통해 스트림 암호화부로 전송되면, 스트림 암호화부는 전송된 키코드 입력정보를 암호화하지 않고 컴퓨터측 송수신 제어부를 통해 컴퓨터 연결부를 거쳐 키보드 장치관리자로 전송하는 단계를 포함하는 것을 특징으로 하는 키코드 입력정보의 보안화 방법.

【청구항 9】

제 8항에 있어서, 상기 비밀키를 이용한 복호화 기능을 컴퓨터 시스템의 상기 키코드 장치관리자가 갖거나, 운영체제가 갖거나 및/또는 응용프로그램이 갖는 것을 특징으로 하는 키코드 입력정보의 보안화 방법.

【청구항 10】

제 8항에 있어서, 키보드 장치관리자와 응용프로그램간, 및 키보드 장치관리자와 응용프로그램간에는 복호화된 자료를 획득하기 위한 프로토콜이 있는 것을 특징으로 하는 키코드 입력정보의 보안화 방법.

【청구항 11】

제 8항에 있어서, 보안모드 설정이 컴퓨터 시스템의 응용프로그램으로부터의 명령에 의한 것이면서 동시에 보안을 요하는 자료의 저장에 관한 것일 때는, 주처리부가 비밀번호의 입력 요청 명령을 컴퓨터 시스템에 전송한 후, 키보드측 송수신 제어부로부터 수신한 비밀번호와 컴퓨터측 송수신 제어부로부터 수신한 보안 자료를 세이프 메모리부로 전송하며, 세이프 메모리는 수신한 자료를 비밀번호를 이용하여 암호화한 후 저장하고,

반면에 보안모드 설정이 컴퓨터 시스템의 응용프로그램으로부터의 명령에 의한 것이면서 동시에 보안 자료의 획득에 관한 것일 때, 주처리부는 비밀번호의 입력 요청 명령을 컴퓨터 시스템에 전송한 후, 키보드측 송수신 제어부로부터 수신한 비밀번호를 세이프 메모리부로 전송하며, 비밀번호가 올바른 경우 세이프 메모리부는 암호화된 자료를 비밀번호를 이용하여 복호화한 후에 주처리부로 전송하고, 비밀번호가 올바르지 않을 경우 세이프 메모리부는 암호화된 자료를 복호화하지 않는 단계를 더 포함하는 것을 특징으로 하는 키코드 입력정보의 보안화 방법.

【요약서】

【요약】

본 발명은 키보드로부터의 키코드 입력정보를 안전하게 컴퓨터 시스템으로 전달하는 보안 어댑터와 그것을 포함한 컴퓨터 보안 시스템에 관한 것으로서, 키보드 또는 컴퓨터 시스템으로부터의 보안모드 설정 명령을 받은 경우에는 키보드로부터의 키코드 입력정보를 암호화하여 컴퓨터 시스템에 전달하고 보안모드 해제 명령을 받거나 보안모드 해제 상태에서는 키보드로부터의 키코드 입력정보를 암호화하지 않고 컴퓨터 시스템으로 전달하는 구성으로 되어있다. 또한, 별도로 보안을 요하는 자료의 저장 및 처리를 필요로 하는 경우에는, 사용자가 올바른 비밀번호를 입력할 때에만 자료를 암호화 내지 복호화할 수 있고 별도로 비밀번호를 저장하지 않는 세이프 메모리부를 부가할 수 있다. 본 발명의 보안 어댑터 및 이를 포함한 컴퓨터 보안 시스템을 사용하면, 인터넷이나 모뎀통신 등과 데이터 네트워크 상에서 사용하여 증권거래, 인터넷 뱅킹, 사이버 거래 등을 함에 있어서, 제3자가 해킹 등의 방법으로 컴퓨터 시스템에 침입하여 사용자의 비밀자료를 도용하는 것을 막을 수 있다.

【대표도】

도 1

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 February 2001 (08.02.2001)

PCT

(10) International Publication Number
WO 01/10079 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/KR00/00811

(22) International Filing Date: 27 July 2000 (27.07.2000)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
1999/31145 29 July 1999 (29.07.1999) KR

29 Mar 01 / 20 mos

(71) Applicant *(for all designated States except US)*: **SAFE TECHNOLOGY CO., LTD.** [KR/KR]; 48-18 Union Building, 4F, Songpa-Dong, Songpa-Gu, Seoul 138-070 (KR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LEE, Jong, Woo** [KR/KR]; 101-901, Hansung Apt., 698-2, Pung-duckchun-ri, Suji-eub, Yongin-si, Kyeongki-do 449-840 (KR).

(74) Agent: **SOHN, Chang, Kyu**; 401 In-bong Building, 640-21, Yoksam-dong, Kangnam-gu, Seoul 135-080 (KR).

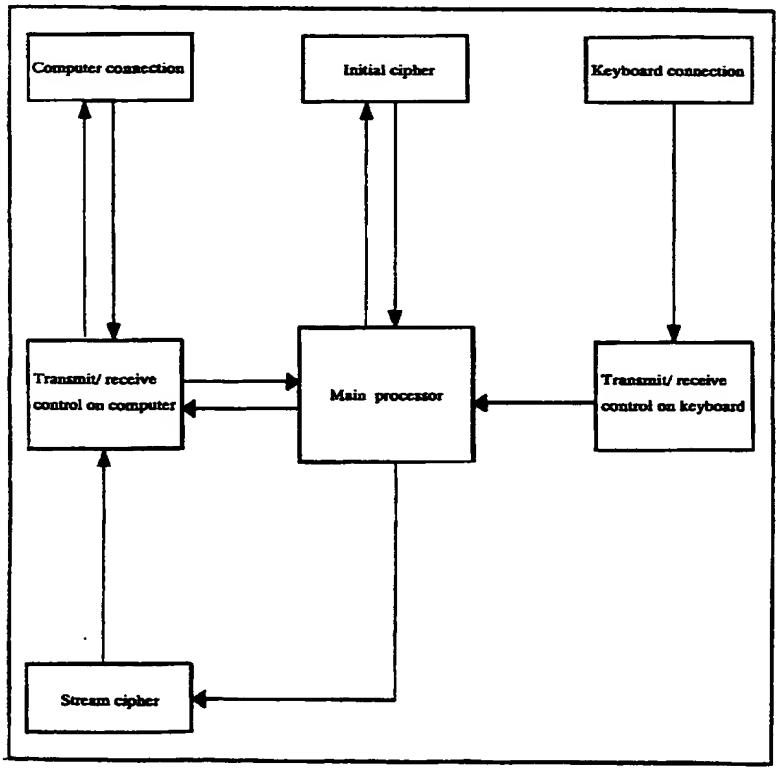
(81) Designated States *(national)*: CN, JP, KR, RU, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ADAPTER HAVING SECURE FUNCTION AND COMPUTER SECURE SYSTEM USING IT



(57) Abstract: A secure adapter and a secure computer system including thereof to safely transfer the key code input information from the keyboard to the computer system. The invention enables transferring the key code input information after encrypting it only when the secure mode setup command is received from the keyboard or the computer system, and transfer the information from the keyboard to the computer system without encryption if the secure mode clearing command is received or under the secure mode clear state. Also, if storage and processing of the data requires special secure handling, the data can be encrypted and decoded only when the user enters correct password, and safe memory which does not store separate password may be added. If the secure adapter and the computer secure system employing thereof of the present invention is used, it is possible to prevent a third person from intruding into the computer system by hacking and stealing user's secrete data, for stock exchange, Internet banking, cyber transactions and other communications over the Internet, modem communications or network data exchange.

WO 01/10079 A1

ADAPTER HAVING SECURE FUNCTION AND COMPUTER SECURE SYSTEM USING IT

Technical Field

This invention relates to adapter ("secure adapter"), to be installed and used between a computer system and a keyboard, which provides security function, and secure computer system using thereof, in particular, to configuration for transferring input information from keyboard to computer system in secure mode by encrypting the data, and for transferring information to computer system in clear mode without encryption.

Background Art

Development of computers and rapid growth of information exchange and communications over Internet has opened the way for quick and easy access to information. In particular, Internet brings a representative paradigm of creating informational environment for individuals, business and e-trade. Internet features openness and conformity, and surmounts difficulties in exchanging and sharing information resources whether used by an individual or a company, whereas the basic drawback of the Internet with respect to information protection and communication safety has been putting serious obstacles. Thus, what is needed is information secure system, which is operable for each service type or application whether communication

Thus, the object of the present invention is to solve the above problems in full and to tackle related technical issues.

That is, the object of the present invention is to prevent information (data) from being drained by other persons using methods not intended by user, such as hacking, enabling the user setting up a secure connection between the computer system and the keyboard for entering data from the keyboard into the computer system .

Also, in the case of with additional safe memory, since the data can be encrypted/decoded only when the user supplies password, and the encryption password is not stored or preserved separately, the present invention can cope with such problems as reproduction and can deal with storing and processing of the data which requires secure handling.

Summary of Invention

To achieve the aforementioned objects, the present invention, which is an adapter to transfer key code input information from the keyboard to the computer system, is configured to transfer the key code input information from the keyboard to the computer system after encrypting it only when the secure mode setup command is received from the keyboard or the computer system, and to transfer the information from the keyboard to the computer system without encrypting the data if the secure mode clear command is received or when in the clear secure mode state.

At the secure mode, the encrypted key code input information may be the

a transmit/receive control on the keyboard to control communication with the keyboard;

a main processor to create a secrete key, to perform secure mode setup/clearing according to the secure mode commands, and to exchange the data between the computer system and the keyboard;

an initial cipher to encrypt the secrete key transferred from the main processor with the secure key from the computer system and then transmit the encrypted secret key to the computer system when the secure mode is set up; and,

a stream cipher to encrypt the key code input information with the secrete key from the main processor and then to transmit the encrypted information to the computer system when the secure mode is set up.

Said transmit/receive control on the computer writes all information to be transmitted on the input buffer first so that the control program transmits it at a proper time, and all received messages are written on the input buffer and can be used in other modules.

Said transmit/receive control on the keyboard transmits the key code input information from the keyboard to the main processor, all commands transmitted are written on the buffer and this module transmits them at a proper time.

Said stream cipher encrypts information transmitted from the main processor with the secrete key. While each different encryption function is applied because bits or characters of a plain text are encrypted, and thus different encryption function is applied and respective plain text bit is encrypted irregardless of other bits for stream cipher,

secrete key was not performed normally. The secure mode indication lamp is not only installed on the secure adapter, but on the front of the computer body, the keyboard or on the monitor as the case may be. If necessary, a small indicator (i.e., an icon type, etc.) can be displayed on the setup screen on the monitor to prompt whether the secure mode is set up or not.

Depending on the case, safe memory interworking with the main configuration of the secure adapter may be added. Said safe memory operates under the secure mode that an application program executed on the computer system established in necessary case, and is used for storing and processing encrypted data which requires separate security handling.

More specifically, said safe memory comprises:

a safe memory interface to transmit a password transmitted from the main processor, or the password and the data which requires security ("secure data"), to an encryption/key operation processor, and to transmit the data received from a decoder to the main processor;

an encryption/key operation processor to convert the password to the key ("the safe key"), and then, if the secure data is not received together with the password from the safe memory interface, to transmit the safe key to the decoder and to encrypt the password with the safe key by encryption algorithm and calculate the integrity identification value of the encrypted password ("password integrity identification value") and then to transmit the password integrity identification value to a comparison/processor, and, if the secure data is received together with the password from the safe memory interface, to encrypt the secure data with the safe key and

password as the password used for storing the encrypted data. Whether the correct password is entered is acknowledged as valid access only when values are the same after comparing the "password integrity identification value" stored in the encrypted data of the data storage memory with the "password integrity identification value" calculated after encryption with the safe key converted from the newly entered password.

Therefore, the safe key transferred from the encryption/key operation processor to the decoder is temporally stored on the buffer of the decoder and then the key is deleted from the buffer by the command from the comparison/processor, where the stored "password integrity identification value" and the "password integrity identification value" calculated from the newly entered password are not the same, as the result of execution of the comparison/processor.

The conversion of password to a safe key may be executed using various known methods such as hash function or polynomial algorithms. Representative examples are the MAC hash function, the MDC hash function, the MD4 hash function, the MD5 hash function, the SHA hash function, the CRC algorithm, and so on.

The integrity identification protects data against hacker's active attacks because it is used as a means to identify the person who performs the access. As a method to identify the integrity, various known algorithms described above can be used, in particular Cyclic Redundancy Checking (CRC) algorithm is preferred. In transmitting the data of K bits, the CRC algorithm transmits the data of k+n bits by dividing the transmitted data into n+1 bit patterns and adding the remaining of n bits length occurred

enter data is correct, while the "encrypted data integrity identification value" being used to identify whether the encrypted data is stored without errors or with errors during storage. That is, it is possible to identify the above by repeatedly encrypting the decoded data with the safe key, calculating the integrity identification value of the encrypted data, and comparing the value with the encrypted data integrity identification value written on the data storage memory. Therefore, it is possible to confirm whether errors occurred in storing or decoding the encrypted data, by adding a separate module that can execute such a function or adding such a function to the basic configuration module.

On the other hand, if each different password is used in storing the multitude of encrypted data at the same time or several times to the data storage memory, a different "password integrity identification value" is stored respectively for the encrypted data. That is to say, passwords may be set differently in storing data, and thus may be specific to the type of encrypted data. Accordingly, if necessary, it is possible to establish the password integrity identification value of the encrypted data stored on the data storage memory depending on the type of encrypted data. In the drain process of the encrypted data, all encrypted data with the same "password integrity identification value" are decoded.

The encryption algorithm used in the safe memory may differ from the encryption algorithm used in the stream cipher of the secure adapter.

The present invention also relates to the computer security system, which comprises the secure adapter, the keyboard and the computer system.

misuse the external interface of the keyboard for hacking purposes.

Referring now to the Fig.3, an example that the computer system can be executed under Microsoft Windows 98 and the keyboard manager has the decoding function is described below. However, in addition to Windows 98, corresponding protocols are applicable for Windows 2000, Windows/NT, Unix, Linux and so on.

When the computer system is operated, the keyboard manager makes and sends the secure key to the secure adapter. Then the manager receives the secrete key encrypted by the secure key from the secure adapter in secure mode, and then receives key code input information encrypted by the secrete key from the secure adapter. The encrypted key code input information received from the secure adapter by the keyboard manager is not immediately decoded, but stored in a location of the keyboard manager or the computer system and only the signal that any key code is pressed is sent to the application program interface by the operating system.

On the one hand, when an application program needs to examine the transferred key code during operation, the application program interface interrupts the code and requests decoding of the key code first pressed to the keyboard manager. Then the keyboard manager transfers the stored encrypted key code input information to the application program interface after decoding it with the stored secrete key, and then the application program interface returns the decoded information to the application program as the result of examination.

With reference, if booting process of the computing system of the present

main processor and then the main processor receives and transfers the data to the safe memory interface. If the safe memory interface transfers password and the secure data to the encryption/key operation processor, the encryption/key operation processor converts the password to the safe key and encrypts the secure data and the password, using the safe key. On the other hand, the encryption/key operation processor calculates the CRC values of the encrypted password and the encrypted data, and then transmits the "encrypted data", the "password CRC value" and the "encrypted data CRC value" to the comparison/processor. The comparison/processor records the information to the data storage memory (refer to the Fig.8).

In the meantime, if the secure mode setup command from the application program is for decoding the stored encrypted information, only the password transferred to the safe memory interface is sent to the encryption/key operation processor. The encryption/key operation processor encrypts password with the safe key after converting the password to the safe key, calculates the CRC value of the encrypted password ("password CRC value"), and then respectively transmits the "safe key" to the decoder, and the "password CRC value" to the comparison/processor. The comparison/processor scans the data storage memory and confirms whether the "password CRC value" stored in the memory is equal to the "password CRC value" received from the encryption/key operation processor. If two CRC values are equal, the comparison/processor receives and transfers the encrypted data from the data storage memory to the decoder. The decoder decodes the encrypted data from the comparison/processor with the safe key, and deletes the safe key after transmission of the data to the safe memory interface. If two values are not equal, the comparison/processor deletes the safe key stored on the decoder buffer and transmits

encrypting the key code input information with the secrete key and transferring the encrypted information to the keyboard manager through computer connection by the transmit/receive control on the computer;

computer system decoding the encrypted information using the secrete key;

main processor transferring the secure mode clearing command to the stream cipher when the secure mode clearing command is transferred from the keyboard or the computer system to the main processor of the secure adapter; and

when secure mode is cleared, the stream cipher transferring the transferred key code input information to the keyboard manager through the computer connection by the transmit/receive control on the computer without encryption, if the key code input information of the keyboard is transferred to the stream cipher through the transmit/receive control on the keyboard after passing through the keyboard connection.

Where the safe memory is incorporated into the main configuration of a secure adapter, the configuration further comprises the step of: main processor transferring the password from the transmit/receive control on the keyboard and the secure data from the transmit/receive control on the computer to the safe memory after the main processor transfers the password input request command to the computer system, and safe memory encrypting and then storing the received data using the password, if secure mode setup is made by the command from the application program of the computer system and also for data storage requiring security; but

main processor transferring the password from the transmit/receive control on the keyboard to the safe memory after the main processor transfers the password input request command to the computer system, and safe memory decoding the encrypted data with the password and then transferring the decoded data to the main processor

computer connection by the transmit/receive control of the computer after encrypting the key code input information, using the secrete key transmitted from the main processor. The process to handle the encrypted key code input information, transferred to the keyboard manager, in the computer system is referred to the details described before on the Fig.3 basis.

If the secure mode clearing command is directed from the computer system or the keyboard, the clear command is transferred to the main processor and the stream cipher by the transmit/receive control on the computer or the transmit/receive control on the keyboard. The main processor turns off the secure mode indication lamp and transfers the secure mode clearing command to the stream cipher. Thereafter, key code values transferred from the keyboard are transferred to the computer system through the computer connection by the transmit/receive control on the computer, without encryption in the stream cipher.

The process to handle the not-encrypted key code input information, transferred to the keyboard manager in the computer system is referred to the details described before on the basis of the Fig.3.

If the secure key is not acquired from the keyboard manager of the computer system during booting the computer, the secure adapter goes in the disabled secure mode, and the main processor sends periodical ON and OFF signals to the secure mode indication lamp. Then, by the keyboard manager and the decoded data transfer protocol, the disabled secure mode state may be notified on the monitor as a message type and so on, and the keyboard input information is transferred to the keyboard manager without

Fig. 6 shows steps for clearing secure mode in the present invention;

Fig. 7 shows steps for processing key code input information under secure mode;

Fig. 8 shows steps for encrypting and storing data in a secure adapter of the Fig. 4; and

Fig. 9 shows steps for decoding stored data in a secure adapter of the Fig. 4.

Industrial Applicability

If the secure adapter and the secure computer system employing thereof of the invention are used, it is possible to prevent third person from intruding into the computer system by hacking and stealing user's secrete data, for stock exchange, Internet banking, cyber transactions and other communications over the Internet, modem communications or for network data transfer.

keyboard;

a main processor to create a secrete key, to perform secure mode setup/clearing according to the secure mode related commands, and to inter-transmit information of the computer system and the keyboard;

an initial cipher to encrypt the secrete key from the main processor with a secure key from the computer system and then to transmit the encrypted secrete key to the computer system, under secure mode; and

a stream cipher to encrypt the key code input information with the secrete key from the main processor and then to transmit the encrypted information to the computer system, under secure mode.

4. The secure adapter according to Claim 1, further comprising a built-in secure mode indication lamp which is ON under secure mode, OFF under cleared secure mode, and periodically blinks under disabled secure mode.

5. The secure adapter according to any one of Claims 1 through 4, further employing safe memory operation under the secure mode set by an application program executed in the computer system, said safe memory comprising:

a safe memory interface to transmit a password transmitted from the main processor, or the password and the data which requires security ("secure data"), to an encryption/key operation processor, and to transmit the data received from a decoder to the main processor;

an encryption/key operation processor to convert the password to the key ("the safe key"), and then, if the secure data is not received together with the password from the safe memory interface, to transmit the safe key to the decoder and to encrypt the

the computer system is for the safe memory.

6. The secure adapter as claimed in Claim 5, where the said integrity identification value is calculated using the CRC algorithm.

7. A computer secure system comprising the secure adapter, the keyboard and the computer system according to any one of Claims 1 through 6, where a separate secure key for entering secure mode setup/clearing command is incorporated in said keyboard and/or the secure mode setup/clearing command can be created by the combination of existing key codes, the computer system has the secure key creation function, the encryption/decoding function with the secrete key and the encryption/decoding function with the secure key, and the keyboard manager with application program interface is included.

8. A method to secure key code input information comprising the steps of:

transferring a secure key created in the keyboard manager of the computer system to the secure adapter in computer booting;

creating a new secrete key in the main processor when the secure mode setup command from the keyboard or the computer system is transferred to the main processor of the secure adapter, and then transferring the secrete key to the initial cipher and the stream cipher of the secure adapter;

encrypting the secrete key with the secure key in the initial cipher and then transferring the encrypted secrete key to the keyboard manager through the computer connection by the transmit/receive control on the computer;

under secure mode, main processor transferring the information to the stream

the keyboard and the secure data from the transmit/receive control on the computer to the safe memory after the main processor transfers the password input request command to the computer system, and safe memory encrypting and then storing the received data using the password, if secure mode setup is made by the command from the application program of the computer system and also for data storage requiring security; but

main processor transferring the password from the transmit/receive control on the keyboard to the safe memory after the main processor transfers the password input request command to the computer system, and safe memory decoding the encrypted data with the password and then transferring the decoded data to the main processor where the password is correct, but not decoding the encrypted data where not correct, if secure mode setup is made by the command from the application program of the computer system and also for acquisition of the secure data.

DRAWINGS

FIG. 1

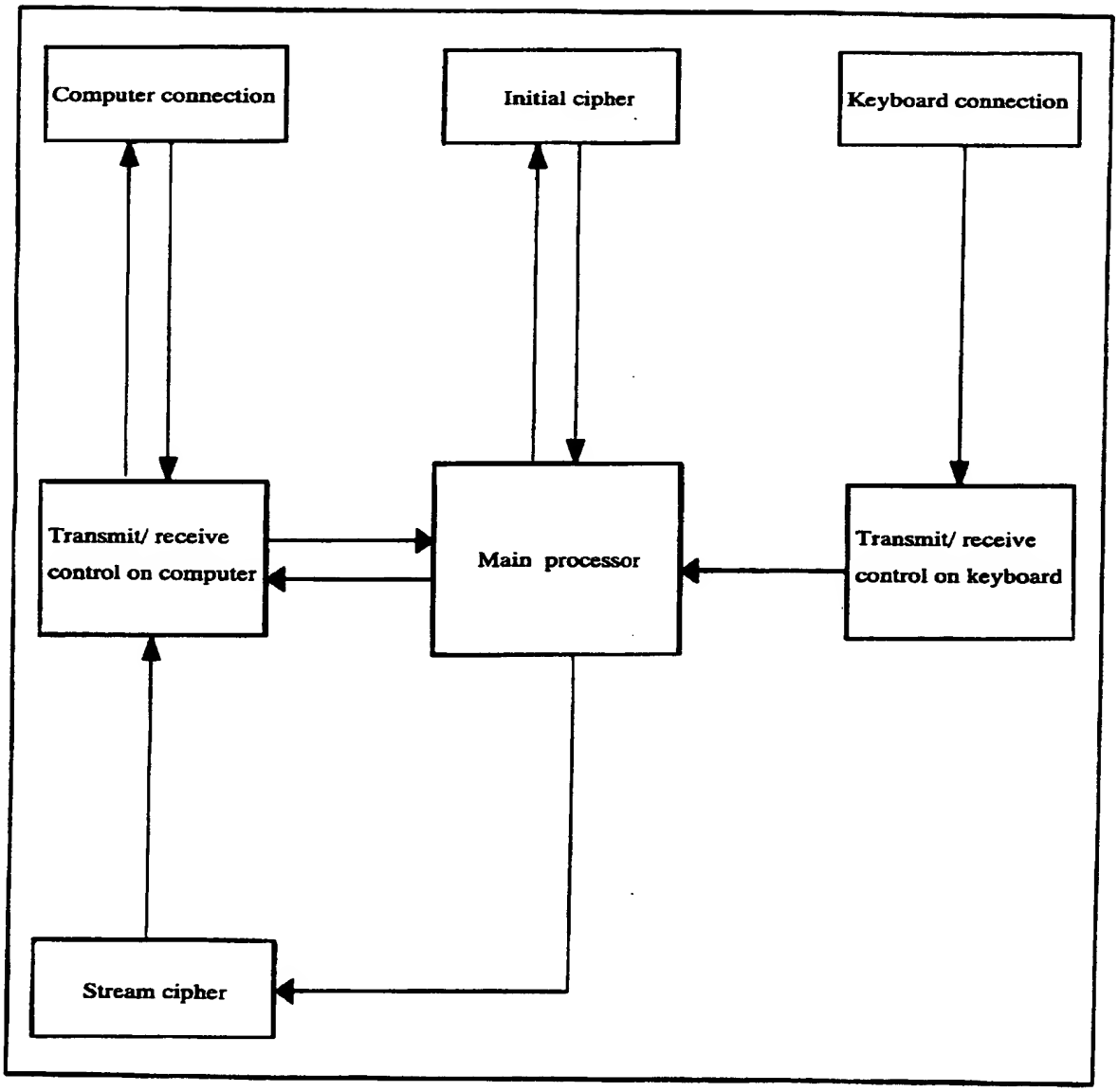


FIG. 2

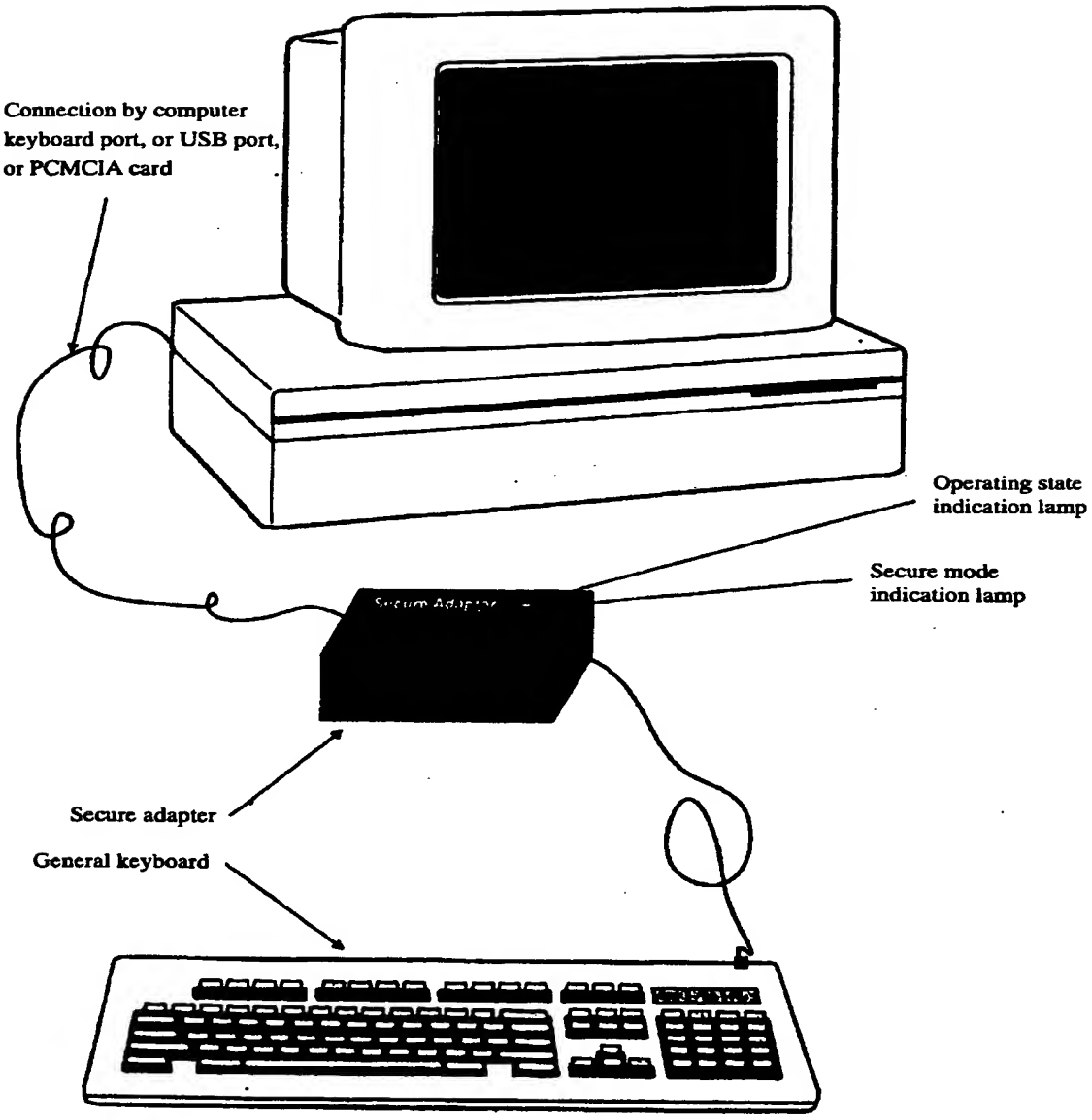

Connection by computer keyboard port, or USB port, or PCMCIA card
Operating state indication lamp
Secure mode indication lamp
Secure adapter
General keyboard

FIG. 3

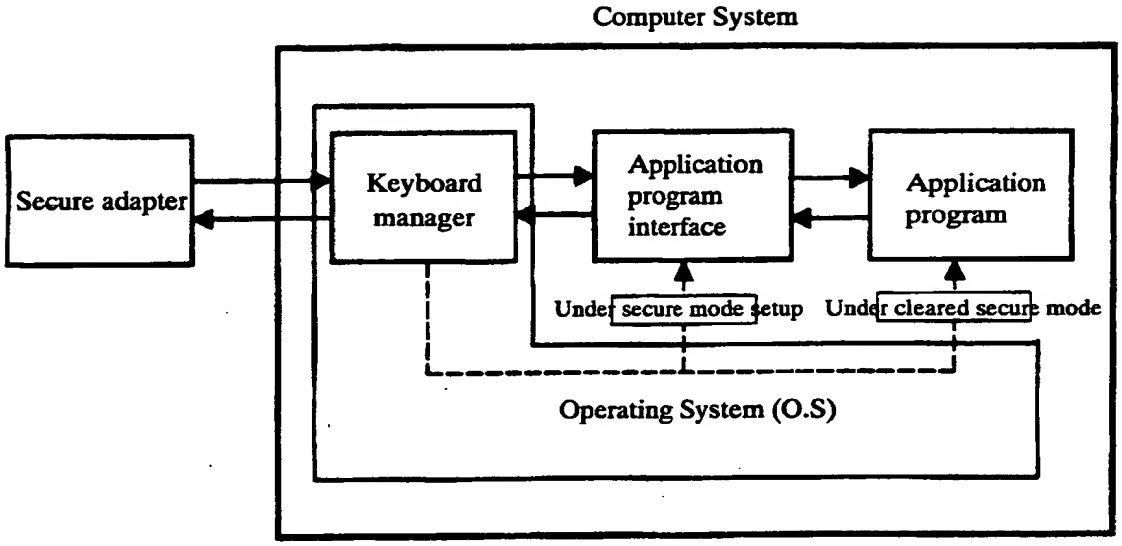

Computer System
Secure adapter
Keyboard manager
Application program interface
Application program
Under secure mode setup
Under cleared secure mode
Operating System (O.S)

FIG. 4

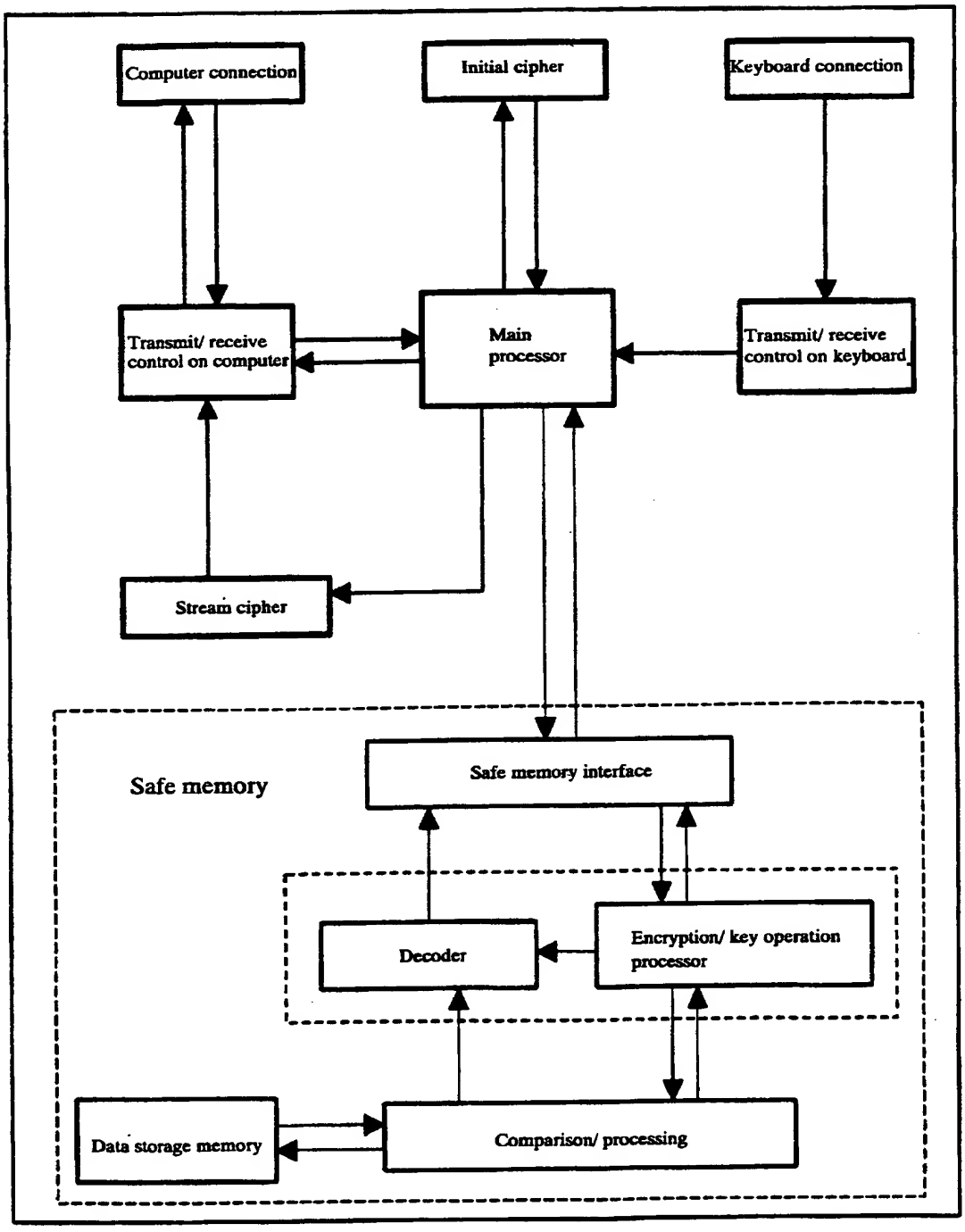

Computer connection
Initial cipher
Keyboard connection
Transmit/ receive control on computer
Main processor
Transmit/ receive control on keyboard
Stream cipher
Safe memory
Safe memory interface
Decoder
Encryption/ key operation processor
Data storage memory
Comparison/ processing

FIG. 5

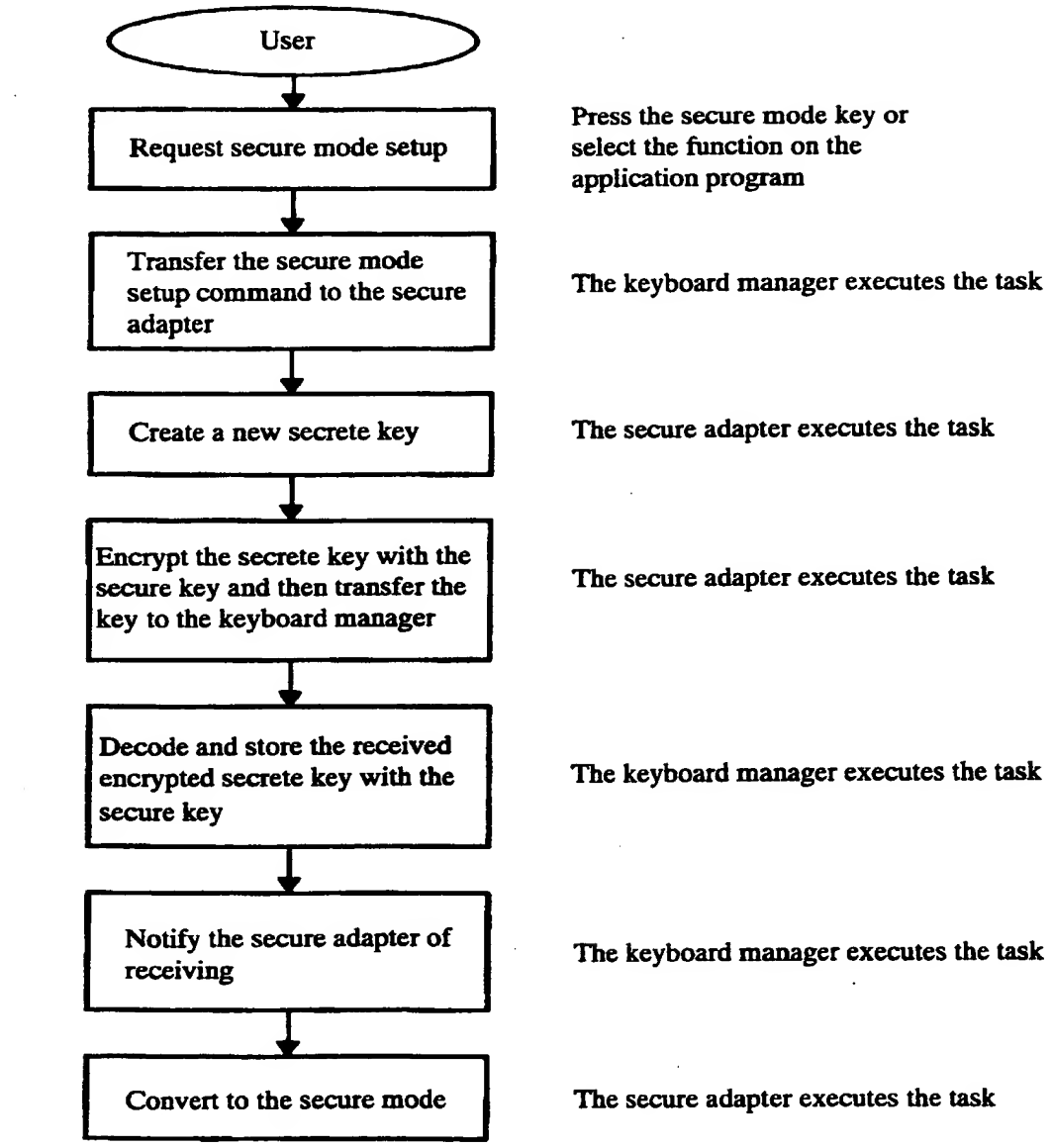

Secure Mode Setup
User
Request secure mode setup
Transfer the secure mode setup command to the secure adapter
Create a new secrete key
Encrypt the secrete key with the secure key and then transfer the key to the keyboard manager
Decode and store the received encrypted secrete key with the secure key
Notify the secure adapter of receiving
Convert to the secure mode
Press the secure mode key or select the function on the application program
The keyboard manager executes the task
The secure adapter executes the task
The secure adapter executes the task
The keyboard manager executes the task
The keyboard manager executes the task
The secure adapter executes the task

FIG. 6

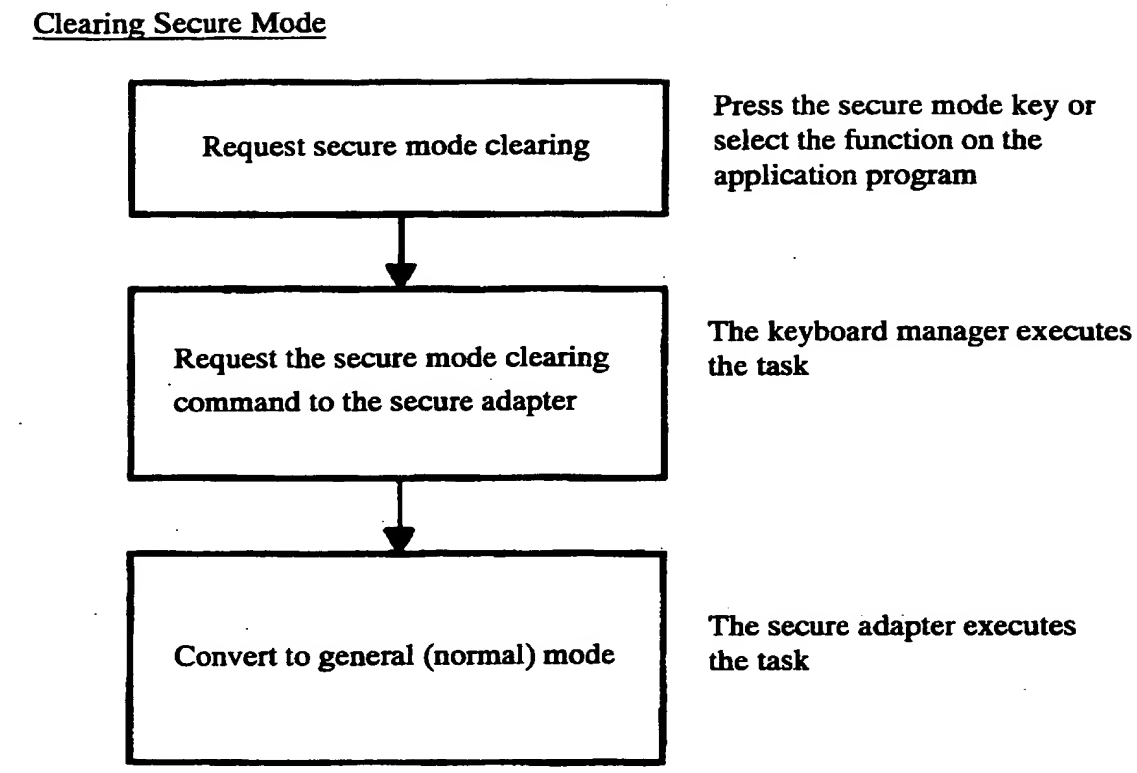

Clearing Secure Mode
Request secure mode clearing
Press the secure mode key or select the function on the application program
Request the secure mode clearing command to the secure adapter
The keyboard manager executes the task
Convert to general (normal) mode
The secure adapter executes the task

FIG. 7

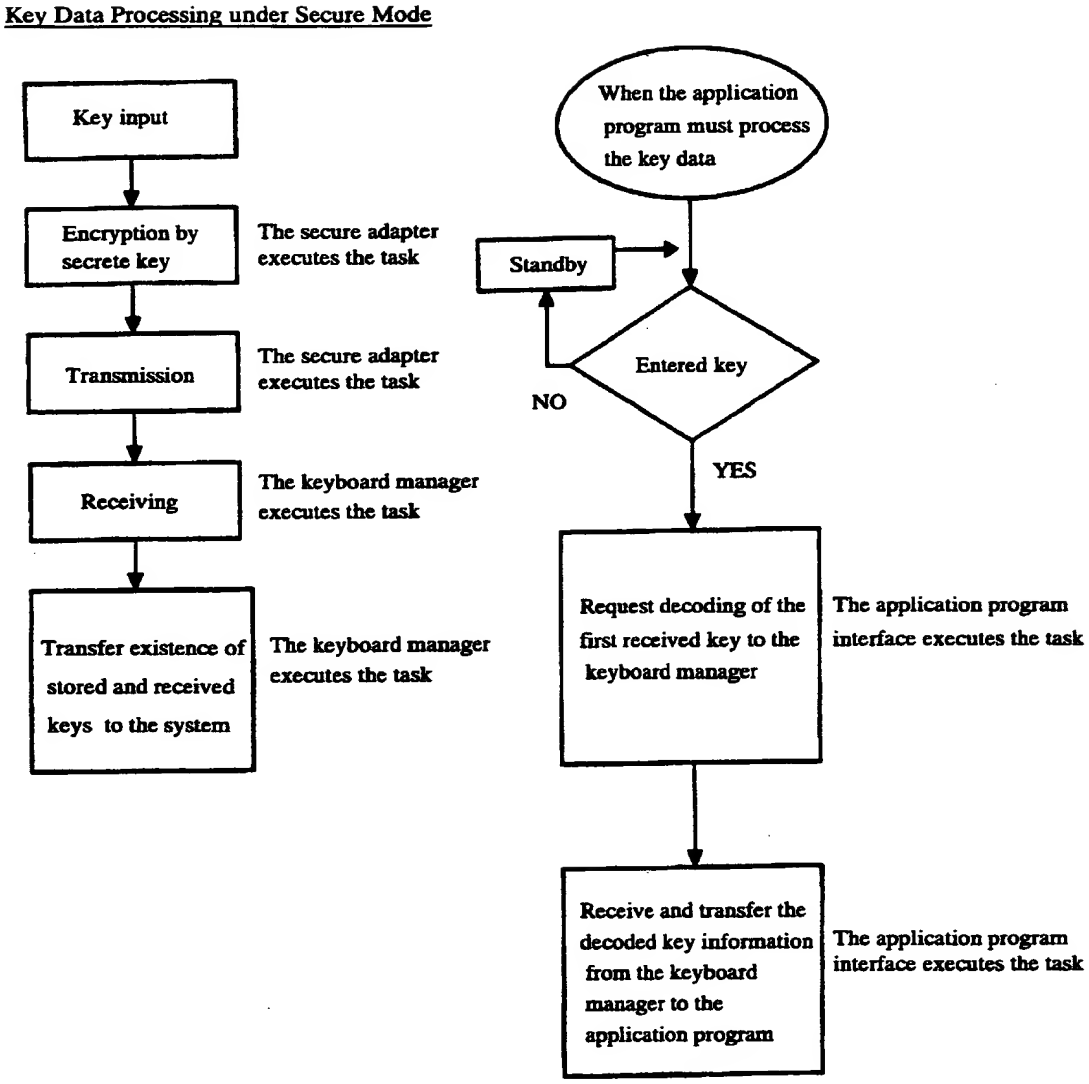

Key Data Processing under Secure Mode
Key input
Encryption by secrete key
The secure adapter executes the task
Transmission
The secure adapter executes the task
Receiving
The keyboard manager executes the task
Transfer existence of stored and received keys to the system
The keyboard manager executes the task
When the application program must process the key data
Standby
Entered key
NO
YES
Request decoding of the first received key to the keyboard manager
The application program interface executes the task
Receive and transfer the decoded key information from the keyboard manager to the application program
The application program interface executes the task

FIG. 8

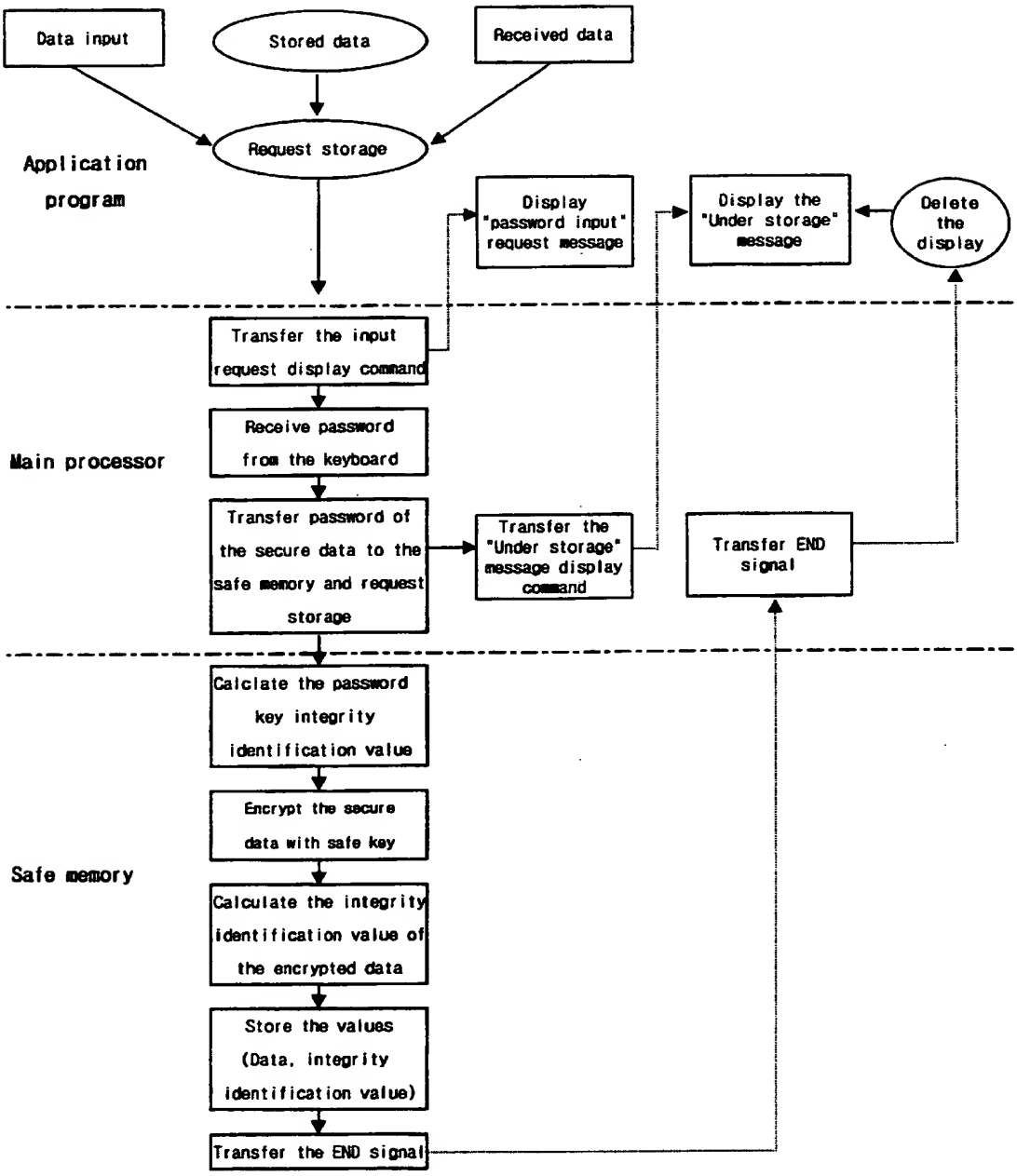
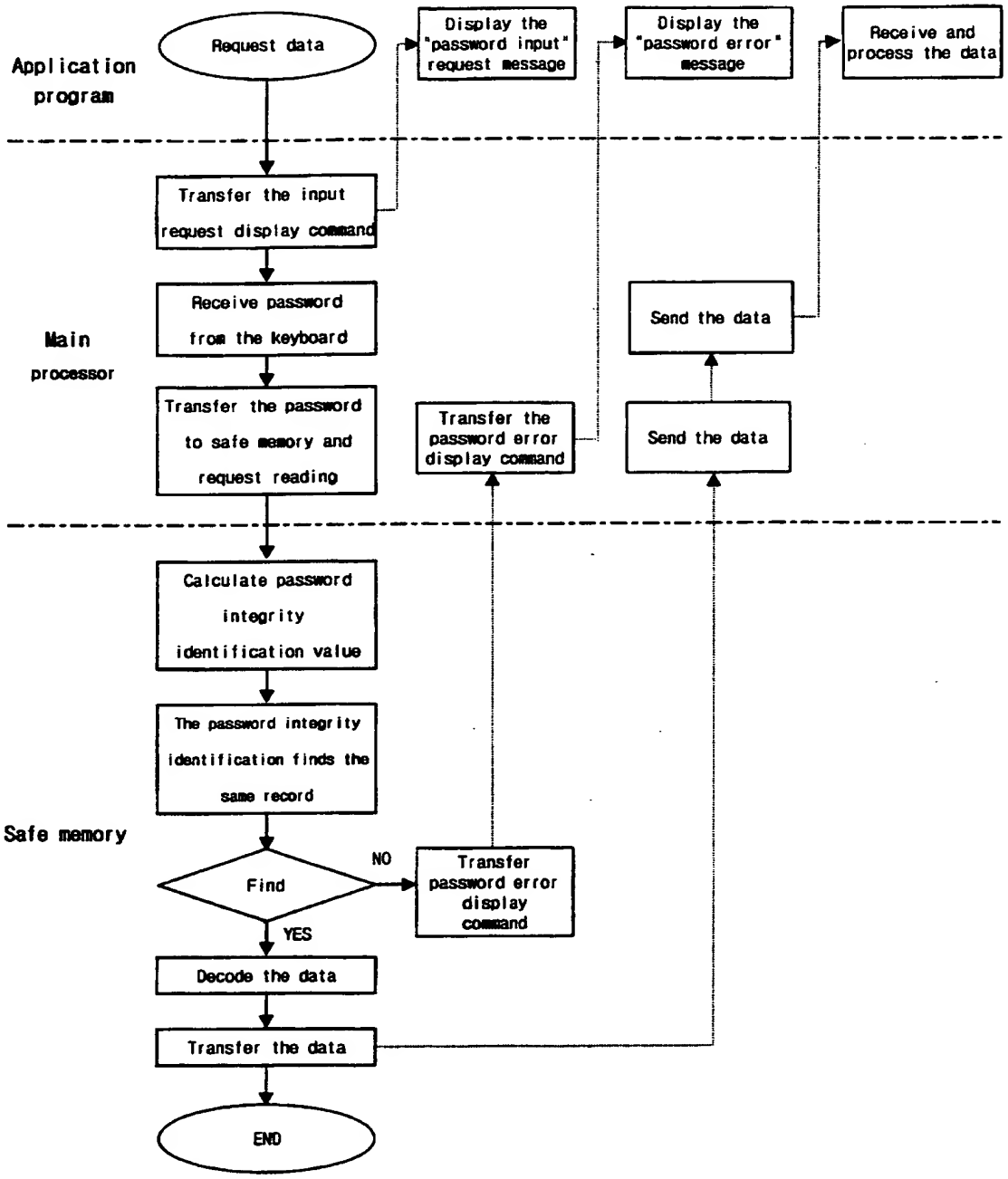

Data input
Stored data
Received data
Request storage
Application program
Display "password input" request message
Display the "Under storage" message
Delete the display
Transfer the input request display command
Receive password from the keyboard
Main processor
Transfer password of the secure data to the safe memory and request storage
Transfer the "Under storage" message display command
Transfer END signal
Calclate the password key integrity identification value
Encrypt the secure data with safe key
Safe memory
Calculate the integrity identification value of the encrypted data
Store the values (Data, integrity identification value)
Transfer the END signal

FIG. 9


Application program
Request data
Display the "password input" request message
Display the "password error" message
Receive and process the data
Transfer the input request display command
Main processor
Receive password from the keyboard
Transfer the password to safe memory and request reading
Send the data
Transfer the password error display command
Send the data
Safe memory
Calculate password integrity identification value
The password integrity identification finds the same record
Find
NO
Transfer password error display command
YES
Decode the data
Transfer the data
END

INTERNATIONAL SEARCH REPORT

international application No.
PCT/KR00/00811

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04L 9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimun documentation searched (classification system followed by classification symbols)
IPC7 G06F1/00, H04L 12/00. H04L 9/00

Documentation searched other than minimun documentation to the extent that such documents are included in the fileds searched
KOREAN PATENTS AND APPLICATIONS FOR INVENTIONS SINCE 1983
KOREAN UTILITY MODELS AND APPLICATIONS FOR UTILITY MODELS SINCE 1983

Electronic data base consulted during the intertnational search (name of data base and. where practicable, search trerms used)
WPI, INSPECT"SECURE ADAPTOR".

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document. with indication. where appropriate. of the relevant passages	Relevant to claim No.
X Y	US 5388156 A (IBM CORP.) 7 FEB. 1995(07.02.1995) abstract. fig8 page 8, lines 21 to 33	1-2 3-4, 8-10
X Y	KR 97-06392 B (IBM CORP) 28 APR. 1997(28.04.1997) fig4. pages 7 to 8	1-2 3-4, 8-10
Y	US 5550984 A (MATSUSHITA ELECTRIC CORP.) 27 AUG. 1996(27.08.1996) page5, lines 12 to 44	1-3, 8-10
Y	US 5214429 A (R.E.T.S SALES AND SERVICE INC.) 25 MAY 1993(25.05.1993) page3, lines 9 to 18	1-3, 8-10
A	KR 98-63709 B (IBM CORP.) 7 OCT. 1998(07.10.1998) page14, lines 30 to 40	1-3, 8-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevence
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure. use. exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevence; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevence; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents.such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 SEPTEMBER 2000 (22.09.2000)	25 SEPTEMBER 2000 (25.09.2000)

Name and mailing address of the ISA/KR	Authorized officer
Korean Industrial Property Office Government Complex-Taejon, Dunsan-dong, So-ku, Taejon Metropolitan City 302-701, Republic of Korea	LEE, Son Tack
Facsimile No. 82-42-472-7140	Telephone No. 82-42-481-5667

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR00/00811

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5388156 A	07.02.1995	AU 663551 B2	12.10.1995
		EP 558222 A1	01.09.1993
		JP 2565629 B2	18.12.1996
		KR 9603058 B1	04.03.1996
KR 97-06392	28.04.1997	EP 588471 A3	23.11.1994
		JP 7191776 A2	28.07.1995
		US 5341422 A	23.08.1994
		CA 2099026 A	
18.03.1994			
US 550984 A	27.08.1996	WO 9618253 A1	
13.06.1996			
		JP 9505719 T	
03.06.1997			
		EP 744107 A1	
27.11.1996			
		AU 2820295 A1	
26.06.1996			
US 5214429 A	25.05.1993	NONE	
KR 98-63709	07.10.1998	US 5864666 A	
26.01.1999			
		JP 10200530 A	
31.07.1998			